HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINKI

Tiedekunta/Osasto — Fakultet/Sektion — Faculty	Laitos — Institution — Department
Matemaattis-luonnontieteellinen	Matematiikan ja tilastotieteen laitos

Tekijä — Författare — Author

Henri Ruoho

Työn nimi — Arbetets titel — Title

Hilbertin Nullstellensatz

Oppiaine — Läroämne — Subject

Matematiikka

Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
Pro gradu -tutkielma	Helmikuu 2014	42 s.

Tiivistelmä — Referat — Abstract

Tutkielmassa esitetään kolme erilaista keinoa todistaa Hilbertin Nullstellensatzin heikko muoto ja tarkastellaan lähestysmistapojen eroavaisuuksia. Tämän jälkeen Nullstellensatzin vahva muoto johdetaan heikosta muodosta käyttäen radikaaleja ja Rabinowitschin keinoa. Lopuksi esitellään joitakin algebrallisen geometrian peruskäsitteitä, joihin Nullstellensatz kytkeytyy ja käydään läpi esimerkkejä tuloksen soveltamisesta.

Avainsanat — Nyckelord — Keywords

Algebrallinen geometria, Hilbert, Nullstellensatz, varisto, polynomi

Säilytyspaikka — Förvaringsställe — Where deposited

Kumpulan tiedekirjasto

Muita tietoja — Övriga uppgifter — Additional information

Henri Ruoho

Hilbertin Nullstellensatz

Pro Gradu -tutkielma

Matematiikan ja tilastotieteen laitos
Helsingin yliopisto

26. helmikuuta 2014

Sisältö

Luku 1

Johdanto

Yksi 1800- ja 1900-lukujen vaikutusvaltaisimmista ja monialaisimmista matemaatikoista oli saksalaissyntyinen David Hilbert (1862-1943). Hilbert uudisti useita matematiikan alueita ja antoi niiden kehitykselle suunnan tulevien vuosikymmenten ajaksi. Hänet tunnetaan muun muassa invarianttiteorian kehitykselle antamastaan panoksesta, Eukleideen geometrian aksiomajärjestelmän nykyaikaistamisesta ja niin kutsuttujen Hilbertin avaruuksien teoriasta, jonka pohjalta funktionaalianalyysina tunnettu matematiikan haara on sittemmin kehittynyt. Erityisen merkityksellinen on ollut Hilbertin vuonna 1900 esittämä 23:n kohdan lista, johon hän kokosi tuon ajan tärkeimmät ratkaisemattomat matemaattiset ongelmat. Lista on inspiroinut laajalti viime vuosisadan matemaatikkoja ja vaikuttanut voimakkaasti matematiikan kehittymiseen. Vaikutus jatkuu vieläkin, sillä osa ongelmista on edelleen ratkaisematta.

Hilbertin tuotteliaisuuden ja vaikutusvaltaisuuden seurauksena hänen nimeään kantavia käsitteitä ja tuloksia on tänä päivänä kymmeniä. Näistä tämä työ keskittyy vain yhteen, Hilbertin Nullstellensatziin.

Gaussin 1800-luvun alussa todistama algebran peruslause antoi aikanaan merkittävän yhteyden algebran ja geometrian välille. Sen mukaan tavallinen $\mathbb{C}$-kertoiminen polynomi määräytyy yksinomaan juurtensa perusteella. Toisin sanoen algebrallinen olio määräytyy geometrisesta oliosta, ja toisin päin. Hilbertin vuonna 1900 todistama Nullstellensatz yleistää tätä yhteyttä useampaan ulottuvuuteen. Tulos on tärkeydessään algebrallisen geometrian kulmakiviä.

Tässä työssä esitetään kolme erilaista todistusta Nullstellensatzin heikolle versiolle ja analysoidaan lähestymistapojen eroavaisuuksia. Seuraavaksi varsinainen Nullstellensatz johdetaan heikosta muodosta käyttäen Rabinowitschin keinoa, jota varten täytyy ensin käsitellä radikaalien ominaisuuksia. Tämän jälkeen tarkastellaan muutamaa esimerkkiä kirjallisuudesta löytyvistä, vaih-

toehtoisista Nullstellensatzin muotoiluista. Näistä erityisesti Lause 6.5 sivulla 35 on tutustumisen arvoinen yleisyytensä vuoksi. Työn viimeisessä osiossa esitellään joitakin algebrallisen geometrian alkeiskäsitteitä, joihin Nullstellensatz kytkeytyy ja käydään läpi eräitä seurauslauseita sekä käytännön esimerkkejä.

Luku 2

Aluksi

2.1 Peruskäsitteitä

Oletan lukijan tuntevan algebran peruskäsitteet siinä laajuudessa kun ne algebran peruskursseilla esitetään. Selvyyden vuoksi tässä osiossa määritellään työssä useimmin tarvittavia käsitteitä, jotka löytyvät tarkemmin esimerkiksi lähteestä [4].

Rengas tarkoittaa tässä työssä kommutatiivista, ykkösellistä rengasta, ellei toisin mainita. Renkaan alirengas sisältää aina ykkösalkion ja renkaiden välinen homomorfismi säilyttää sen. *Kokonaisalue* on rengas, jossa ei ole nollanjakajia, eli jossa kahden alkion tulo on nolla vain jos ainakin toinen alkioista on nolla. Renkaan ideaalia sanotaan aidoksi, jos se ei ole koko rengas.

Renkaan alkio a on jaollinen alkiolla b, mikäli jollain c pätee $a = bc$. Sanotaan myös, että b jakaa alkion a. Jos tämä pätee vain silloin, kun $b = 1$ tai $c = 1$, niin a on *jaoton*. Jos sen sijaan $ab = 1$ joillakin renkaan alkoilla a ja b, niin a on kääntyvä eli *yksikkö*.

Renkaan aitoa ideaalia sanotaan *maksimaaliseksi*, jos se ei sisälly mihinkään toiseen aitoon ideaaliin. Renkaan ideaali on *alkuideaali*, jos siihen kuuluvan tulon tekijöistä ainakin yksi kuuluu aina ideaaliin. Maksimaaliset ideaalit ovat siis alkuideaaleja. Jos alkuideaali sattuu olemaan *pääideaali*, eli yhden alkion virittämä, sen virittäjää sanotaan *alkualkioksi*.

Rengasta, jonka jokainen ideaali on pääideaali, sanotaan *pääideaalirenkaaksi*. Voidaan todistaa, että pääideaalirenkaan alkuideaalit ovat maksimaalisia (esim. [4]).

Kokonaisalue on *faktoriaalinen*, mikäli jokainen sen alkio on esitettävissä jaottomien alkioiden tulona järjestystä vaille yksikäsitteisellä tavalla. Jos kokonaisalueen kaikki ideaalit ovat pääideaaleja, se on faktoriaalinen, kuten esimerkiksi lähteessä [5] todistetaan.

Kunta on rengas, jonka jokainen nollasta poikkeava alkio on kääntyvä. Kunnalle käytetään tässä työssä ensisijaisesti symbolia K. Jos K ja L ovat kuntia ja $K \subset L$, niin L on kunnan K *laajennos* ja K puolestaan kunnan L alikunta. Silloin L on joka tapauksessa K-vektoriavaruus, jonka dimensio määritellään kyseisen *laajennoksen asteeksi*. Laajennosta sanotaan äärelliseksi tai äärettömäksi sen mukaan, onko sen aste äärellinen vai ei.

Kunnan $K \subset L$ *äärellisesti viritetty laajennos* $K(a_1, \ldots, a_n)$ on pienin kunta, joka sisältää kunnan K ja alkiot $a_1, \ldots, a_n \in L$. Äärellinen laajennos on äärellisesti viritetty (ks. [4]), muttei välttämättä toisinpäin: esimerkiksi $\mathbb{Q}(\pi)$ on äärellisesti viritetty ääretön laajennos.

Jos K ja L ovat kuntia ja $K \subset L$, niin alkiota $a \in L$ sanotaan *algebralliseksi* kunnan K suhteen, mikäli se on jonkin K-kertoimisen polynomin juuri. Esimerkiksi $\sqrt{2} \in \mathbb{R}$ on algebrallinen kunnan $\mathbb{Q}$ suhteen, π ei ole. Jos kaikki kunnan L alkiot ovat algebrallisia kunnan K suhteen, laajennosta $K \subset L$ sanotaan algebralliseksi. Esimerkiksi $\mathbb{C}$ on kunnan $\mathbb{R}$ algebrallinen laajennos.

Kunta K on *algebrallisesti suljettu*, jos sillä ei ole aitoja algebrallisia laajennoksia. Tämä on yhtäpitävää sen kanssa, että kaikilla K-kertoimisilla polynomeilla on juuri kunnassa K. Kunnan K *algebrallinen sulkeuma* on sen algebrallinen laajennos, joka on algebrallisesti suljettu. Esimerkiksi $\mathbb{C}$ on kunnan $\mathbb{R}$ algebrallisesti suljettu algebrallinen laajennos, joten se on kunnan $\mathbb{R}$ algebrallinen sulkeuma.

Kokonaisalueen sisältävistä kunnista pienintä kutsutaan sen *osamääräkunnaksi*. Sen konstruktio on erikoistapaus lokalisaatiosta, ks. sivu 6.

2.2 Algebrat

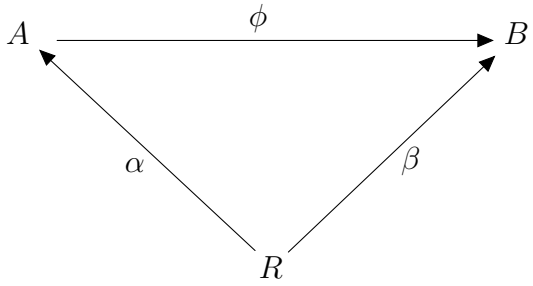
Jos R on rengas, niin R-*algebra* on mikä tahansa rengas A yhdessä homomorfismin $\alpha\colon R \to A$ kanssa. Homomorfismin avulla voidaan määritellä "skalaarikertolasku" asettamalla $r.a = \alpha(r)a$ kaikilla $r \in R$ ja $a \in A$. Toisin sanoen algebra on kerroinrenkaalla varustettu vaihdannainen rengas, siinä missä moduli on kerroinrenkaalla varustettu vaihdannainen ryhmä. Merkintää $r.a$ käytetään tässä työssä toisinaan selvyyden vuoksi. Yleensä piste (tai α) on tapana jättää merkitsemättä ja kirjoittaa lyhyesti $ra = r.a(= \alpha(r)a)$.

Jokainen rengas R on triviaalisti R-algebra. Huomattavasti tärkeämpi esimerkki on polynomirengas $R[x_1, \ldots, x_n]$, jota usein kutsutaankin polynomialgebraksi.

Algebran (A, α) alirengas $A' \subset A$ on *alialgebra*, mikäli $\alpha R \subset A'$. Esimerkiksi R on polynomialgebran $R[x_1, \ldots, x_n]$ alialgebra.

R-algebrojen (A, α) ja (B, β) välinen kuvaus $\phi : A \to B$ on *algebrahomomorfismi*, mikäli se on rengashomomorfismi ja toteuttaa ehdon $\phi \circ \alpha = \beta$.

Silloin $\phi(r.a) = \phi(\alpha(r)a) = \phi(\alpha(r))\phi(a) = \beta(r)\phi(a) = r.\phi(a)$; kyseessä on siis eräänlainen lineaarisuusehto.



Kuva 2.1: Algebrahomomorfismin tapauksessa kaavio kommutoi

Tarkastellaan R-algebroja (A, α) ja $R[x_1, \ldots, x_n]$. Jos $a_1, \ldots, a_n \in A$, niin voidaan määritellä algebrahomomorfismi $\phi : R[x_1, \ldots, x_n] \to A$, jolla $\phi(x_i) = a_i$ kaikilla $i = 1, \ldots, n$ ja $\phi(r) = \alpha(r)$ kaikilla $r \in R$. Tämä on ainoa homomorfismi, joka toteuttaa yhtälöt $\phi(x_i) = a_i$, sillä jos ϕ ja ψ ovat tällaisia kuvauksia ja $P \in R[x_1, \ldots, x_n]$, $P = \sum_{i=1}^{k} p_i x_1^{q_1} \cdots x_n^{q_n}$ mielivaltainen polynomi, niin

$$\begin{aligned}\phi(P) = \phi(\sum_{i=1}^{k} p_i x_1^{q_1} \cdots x_n^{q_n}) &= \sum_{i=1}^{k} \alpha(p_i)\phi(x_1)^{q_1} \cdots \phi(x_n)^{q_n} \\ &= \sum_{i=1}^{k} \alpha(p_i)\psi(x_1)^{q_1} \cdots \psi(x_n)^{q_n} = \psi(\sum_{i=1}^{k} p_i x_1^{q_1} \cdots x_n^{q_n}) = \psi(P).\end{aligned}$$

Kuva $\operatorname{Im}\phi$ on algebran A alialgebra, koska se on alirengas ja $\alpha R \subset \operatorname{Im}\phi$. Miten kuva $\operatorname{Im}\phi$ liittyy alkioihin a_i? Jos jokin alialgebra sisältää alkiot $a_1, \ldots, a_n$, niin se sisältää myös kaikki kuvan $\operatorname{Im}\phi$ alkiot suoraan määritelmien perusteella. Toisaalta $\operatorname{Im}\phi$ sisältää itsekin alkiot $a_1, \ldots, a_n$, joten se on tällaisista alialgebroista pienin. Siis $\operatorname{Im}\phi$ on alkioiden $a_1, \ldots, a_n$ *virittämä alialgebra*; sille käytetään merkintää $R[a_1, \ldots, a_n]$ (vaikka täsmällisempi merkintä olisi $\alpha(R)[a_1, \ldots, a_n]$).

Seuraava huomio on tarpeen myöhemmin.

Lemma 2.1. *Olkoot A ja B äärellisviritteisiä R-algebroja ja $\phi\colon A \to B$ algebrahomomorfismi. Silloin (B, ϕ) on äärellisviritteinen A-algebra.*

Todistus. Oletetaan, että $A = \alpha(R)[a_1, \ldots, a_m]$ ja $B = \beta(R)[b_1, \ldots, b_n]$ joillakin $a_i \in A$ ja $b_j \in B$. Riittää osoittaa, että $B = \phi(A)[b_1, \ldots, b_n]$. Tehdään tämä näyttämällä sisältyminen kumpaankin suuntaan.

Jos $p \in B$, niin $p \in \phi(\alpha(R))[b_1, \ldots, b_n]$, sillä $\beta = \phi \circ \alpha$. Lisäksi $\alpha(R) \subset A$, joten $p \in \phi(A)[b_1, \ldots, b_n]$. Näin ollen $B \subset \phi(A)[b_1, \ldots, b_n]$ ja toinen suunta on selvä.

Jos $p \in \phi(A)[b_1, \ldots, b_n]$, niin jokainen polynomin p kerroin on jonkin polynomin $p' \in A$ kuva $\phi(p')$. Koska $p' \in \alpha(R)[a_1, \ldots, a_m]$ ja ϕ on homomorfismi, kuva $\phi(p')$ on $\phi(\alpha(R)) = \beta(R)$-kertoiminen alkioiden $\phi(a_1), \ldots, \phi(a_m)$ polynomi. Nämä ovat kuitenkin $\beta(R)$-kertoimisia alkioiden $b_1, \ldots, b_n$ polynomeja, joten myös p on $\beta(R)$-kertoiminen alkioiden $b_1, \ldots, b_n$ polynomi. Toisin sanoen, $p \in B$. □

Tässä työssä äärellisesti viritetyn algebran kerroinrengas R on yleensä aina kunta. Silloin homomorfismi $\alpha\colon K \to K[x_1, \ldots, x_n]$ on injektio eli $\alpha(K) \simeq K$. Alkioiden $a_1, \ldots, a_n$ virittämälle alialgebralle pätee tällöin

$$R[a_1, \ldots, a_n] \overset{\text{määr.}}{=} \alpha(K)[a_1, \ldots, a_n] \simeq K[a_1, \ldots, a_n],$$

eli merkintä $K[a_1, \ldots, a_n]$ on täsmällinen. Kunnan tapauksessa äärellisvirritteistä algebraa $K[a_1, \ldots, a_n]$ sanotaan *affiiniksi algebraksi*. Jos se on lisäksi kokonaisalue, puhutaan *affiinista K-alueesta*.

2.3 Lokalisaatio

Olkoon R rengas $S \subset R$ jokin tulon suhteen suljettu osajoukko. Joukossa $R \times S$ voidaan määritellä relaatio

$$(r, s) \sim (r', s') \quad \Leftrightarrow \quad t(rs' - r's) = 0 \quad \text{jollakin} \quad t \in S.$$

Tällöin $\sim$ on ekvivalenssirelaatio, jonka luokkaa $[(r, s)]_\sim$ merkitään r/s. Rakenne $S^{-1}R = R \times S/\sim$ on rengas, kun laskutoimitukset määritellään kuten rationaaliluvuilla.

Jos $p \subset R$ on alkuideaali, niin $S = R \setminus p$ on tulon suhteen suljettu joukko. Tässä tapauksessa yllä konstruoitua rengasta merkitään R_p ja kutsutaan renkaan R *lokalisaatioksi* alkuideaalin p suhteen. Voidaan nimittäin todistaa, että R_p todella on lokaali rengas, eli sisältää yksikäsitteisen maksimaalisen ideaalin.

Lokalisaation erikoistapauksena saadaan kokonaisalueen osamääräkunta. Jos nimittäin D on kokonaisalue, $S = D \setminus \{0\}$ on tulon suhteen suljettu, joten $S^{-1}D$ voidaan konstruoida. Tätä merkitään $\mathrm{Quot}(D)$ ja kutsutaan kokonaisalueen D osamääräkunnaksi. Se on kunta, koska jos $a/b \neq 0$, niin $a \neq 0$ ja siten $b/a \in \mathrm{Quot}(D)$.

2.4 Zornin lemma ja Krullin lause

Selvyyden vuoksi esitetään vielä lyhyesti kaksi kommutatiivisen algebran perustulosta 1900-luvun alkupuolelta. Kumpikin lauseista on ekvivalentti valinta-aksioman kanssa ZF-joukko-opissa.

Lause 2.2 (Zornin lemma)**.** *Jos osittain järjestetyn joukon jokaisella ketjulla on yläraja, joukosta löytyy maksimaalinen alkio.*

Todistus. Todistuksessa käytetään useimmiten ordinaaleja ja transfiniittista induktiota, ks. esim. [2]. □

Zornin lemma on nimetty itävaltalaisen matemaatikon Max Zornin mukaan. Suoraan siitä tai vaihtoehtoisesti valinta-aksiomasta voidaan todistaa Krullin lause (Wolfgang Krull 1929).

Lause 2.3 (Krullin lause)**.** *Jos R on epätriviaali rengas, sillä on maksimaalinen ideaali.*

Todistus. Olkoon S kaikkien renkaan R aitojen ideaalien kokoelma. Se on sisältymisrelaation suhteen osittain järjestetty joukko. Jos C on jokin ketju joukon S alkioita, niin $\cup C$ on sen yläraja. Zornin lemman nojalla joukossa S on siis maksimaalinen alkio. Se on samalla maksimaalinen ideaali, joten väite pätee. □

Huomautus. Samalla tavalla voidaan todistaa, että jokainen renkaan R aito ideaali sisältyy johonkin maksimaaliseen ideaaliin. Tämä on Krullin lauseen toinen muotoilu.

2.5 Hilbertin kantalause

Vuonna 1888 Hilbert todisti niin kutsutun kantalauseensa. Tuohon aikaan hän tutki vielä invarianttiteoriaa, jonka kehittämiselle kantalause on ollut suureksi avuksi. Tulos yleisti huomattavasti hieman aiemmin todistettuja kannan olemassaoloa käsitteleviä tuloksia, joille P. Gordan ja F. Mertens olivat antaneet panoksensa.

Alla kantalause on muotoiltu tavallisessa yleisyydessään, jossa kerroinrengas on niin sanottu *Noetherin rengas* (Emmy Noether, 1882-1935). Tämä tarkoittaa lyhyesti sanottuna sitä, että renkaan R jokainen kasvava ideaaliketju $I_1 \subset I_2 \subset \ldots$ vakautuu jostakin indeksistä lähtien. Tätä työtä varten riittää tietää, että kunnat ovat Noetherin renkaita.

Lause 2.4 (Hilbertin kantalause)**.** *Olkoon R Noetherin rengas ja $I \subset R[x]$ ideaali. Silloin I on äärellisesti viritetty.*

Todistus. Ks. esim. [5]. □

Hilbertin kantalause on erinomaisen hyödyllinen tulos, mutta tässä työssä se on esitetty lähinnä yleissivistyksen vuoksi. Sitä tarvitaan ainostaan sivulla 34 esitettävän Lauseen 6.2 perusteluun.

Luku 3

Hilbertin Nullstellensatz

Tässä osiossa esitetään kolme todistusta niin kutsutulle Nullstellensatzin heikolle muodolle. Kirjallisuudessa esiintyy vaihtelua sen mukaan millaista muotoilua tulokselle käytetään, mutta sisällöltään tulokset ovat kuitenkin usein samanarvoisia. Työssäni noudatan mielestäni yleisimmin käytössä olevaa muotoilua, joka löytyy esimerkiksi lähteestä [6].

3.1 Esimuoto

Aluksi heikkoa muotoa lähestytään todistamalla tulos, jota nimitän Nullstellensatzin esimuodoksi. Se on verraten helposti todistettava välivaihe, josta Nullstellensatzin heikko muoto seuraa pienellä vaivalla. Esimuoto todistetaan aluksi kahdella tavalla, joita vertaillaan osiossa 4.

Viittausteknisistä syistä esitän Nullstellensatzin esimuodon seuraavaksi, ennen varsinaisia todistuksia.

Lause 3.1 (Nullstellensatzin esimuoto)**.** *Olkoon K algebrallisesti suljettu kunta ja $M \subset K[x_1, \ldots, x_n]$ maksimaalinen ideaali. Silloin M on muotoa $M = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ jollakin $(a_1, \ldots, a_n) \in K^n$.*

3.2 Esimuodon todistus, tapa 1

Ensimmäinen tapa on lähestyä tilannetta äärellisviritteisten algebrojen näkökulmasta. Tämän lähestymistavan kannalta seuraava lemma on erittäin oleellinen.

Lemma 3.2. *Olkoon A jokin K-algebra, missä K on kunta. Jos A on kerroinkunnan suhteen algebrallinen kokonaisalue, niin A on kunta. Toisaalta,*

jos A on kunta ja sisältyy johonkin affiiniin K-alueeseen, niin se on algebrallinen kunnan K suhteen.

Todistus. Oletetaan ensin, että A on algebrallinen kokonaisalue. A on kunta, mikäli sen jokainen nollasta poikkeava alkio $a \in A$ on kääntyvä. Tätä varten riittää näyttää, että jokaisella $a \neq 0$ alialgebra $K[a]$ on kunta.

Tarkastellaan valuaatiokuvausta $K[x] \to A$, $f \mapsto f(a)$, missä $K[x]$ on tavallinen yhden muuttujan polynomialgebra. Tämän kuva $K[a]$ on kokonaisalue, sillä $K[a] \subset A$. Jos $I \subset K[x]$ on kuvauksen ydin, niin $I \neq \{0\}$ alkion a algebrallisuuden nojalla. Suoraan homomorfialauseen perusteella $K[x]/I \simeq K[a]$, joten $K[x]/I$ on kokonaisalue ja siten I on alkuideaali. Koska $K[x]$ on pääideaalirengas, tästä seuraa, että I on maksimaalinen. Niinpä $K[a] \simeq K[x]/I$ on kunta ja erityisesti a on kääntyvä.

Oletetaan sitten, että A on kunta ja sisältyy affiiniin alueeseen $D = K[a_1, \ldots, a_n]$, joillain $a_1, \ldots, a_n \in D$. Oletetaan vastoin väitettä, että on olemassa jokin $a \in A$, joka ei ole algebrallinen. Sovitaan lisäksi yksinkertaisuuden vuoksi, että $a = a_1$. Nyt, mahdollisesti indeksejä järjestelemällä, saadaan muodostettua maksimaalinen vapaa osajono $(a_1, \ldots, a_r)$.

Tarkastellaan äärellisesti viritettyä kuntalaajennosta $L = K(a_1, \ldots, a_r)$, joka määritelmän mukaisesti on pienin alkiot $a_1, \ldots, a_r$ ja kunnan K sisältävä kunta. Toisaalta myös osamääräkunta $\mathrm{Quot}(D)$ sisältää K:n ja mainitut alkiot, joten $L \subset \mathrm{Quot}(D)$.

Jokainen rationaalilauseke $f/g \in \mathrm{Quot}(D)$ voidaan esittää L-lineaarikombinaationa esimerkiksi alkioista $\{1/a_1, \ldots, 1/a_n\}$, koska $(a_1, \ldots, a_r)$ oli maksimaalisesti vapaa osajono. Siis $\mathrm{Quot}(D)$ on kunnan L äärellinen laajennos, eli äärellisulotteinen L-vektoriavaruutena. Valitaan laajennokselle jokin kanta, jonka pituus olkoon m. Jokaisella $b \in \mathrm{Quot}(D)$ translaatio

$$\phi_b : \mathrm{Quot}(D) \to \mathrm{Quot}(D), \qquad \phi_b(x) = bx$$

on L-lineaarinen homomorfismi, joten sillä on valitun kannan suhteen matriisiesitys joukossa $L^{m\times m}$. Nyt voidaan määritellä kuvaus $\phi : \mathrm{Quot}(D) \to L^{m\times m}$ luonnollisesti niin, että ϕ liittää jokaiseen b tätä vastaavan matriisin ϕ_b. Havaitaan, että kaikilla $x, b, b' \in \mathrm{Quot}(D)$

$$\phi_{b+b'}(x) = (b+b')x = bx + b'x = \phi_b(x) + \phi_{b'}(x)$$

ja

$$\phi_{bb'}(x) = (bb')x = b(b'x),$$

joten $\phi(b+b') = \phi(b) + \phi(b')$ ja $\phi(bb') = \phi(b)\phi(b')$ kaikilla $b, b' \in \mathrm{Quot}(D)$.

Tarkastellaan erityisesti matriiseja $\phi(a_i) \in L^{m\times m}$, missä $i = 1, \ldots, n$. Niiden alkiot ovat polynomien osamääriä (koska $L \subset \mathrm{Quot}(D)$), joten voidaan

valita jokin nimittäjien yhteinen monikerta $g \in K[a_1, \ldots, a_r]$, $g \neq 0$. Silloin

$$\phi(a_i) \in K[a_1, \ldots, a_r, g^{-1}]^{m \times m}$$

kaikilla $i = 1, \ldots, n$, eli osamääristä on tavallaan päästy eroon. Koska ϕ säilyttää summat ja tulot, myös kaikki alkioista a_i muodostetut K-polynomit kuvautuvat renkaaseen $K[a_1, \ldots, a_r, g^{-1}]^{m \times m}$. Niinpä

$$\phi(D) \subset K[a_1, \ldots, a_r, g^{-1}]^{m \times m}. \tag{3.1}$$

Affiinilla algebralla $K[a_1, \ldots, a_r]$ on polynomirenkaan rakenne, joten se on faktoriaalinen, eli erityisesti sen alkiolla g on alkutekijähajotelma. Olkoot $p_1, \ldots, p_k$ ne alkutekijät, jotka löytyvät alialgebrasta $K[a_1]$, ja olkoon $p \in K[a_1]$ jokin mielivaltainen jaoton alkio. Joka tapauksessa $p \in A$, koska $K[a_1] \subset A$ oletuksen $a_1 \in A$ nojalla. Silloin myös $p^{-1} \in A$, sillä A on kunta. Niinpä $p^{-1} \in D$ ja on siis mielekästä tarkastella alkiota $\phi(p^{-1})$. Koska $K[a_1] \subset L$, pätee $p \in L$ eli p on skalaari laajennoksessa $\mathrm{Quot}(D)/L$. Niinpä $\phi(p)$ on diagonaalimatriisi, jonka lävistäjäalkio on joka kohdassa p. Silloin myös $\phi(p^{-1})$ on diagonaalimatriisi, lävistäjällään p^{-1}.

Sisältymisen (3.1) perusteella $\phi(p^{-1}) \in K[a_1, \ldots, a_r, g^{-1}]^{m \times m}$, joten edeltävän päättelyn mukaan $p^{-1} = g^{-s} f$ eli $g^s = pf$ jollain $f \in K[a_1, \ldots, a_r]$ ja $s \geq 0$. Niinpä p on alkion g alkutekijä renkaassa $K[a_1]$ eli jonkin alkion $p_1, \ldots, p_k$ K-monikerta. Koska p oli mielivaltainen, tästä seuraa, että jokainen faktoriaalisen renkaan $K[a_1]$ skalaarista poikkeava alkio on jaollinen jollain p_i. Tämä on kuitenkin liikaa vaadittu, sillä esimerkiksi $1 + \prod_{i=1}^{k} p_i$ ei ole jaollinen millään p_i. Saadun ristiriidan nojalla alkuoletus on väärä ja siten A on algebrallinen.

□

Edellisen lemman kumpaakin kohtaa käyttämällä voidaan todistaa varsin helposti seuraava lause, joka tulee käyttöön Nullstellensatzin esimuotoa todistettaessa.

Lause 3.3. *Olkoon K kunta, A ja B K-kertoimisia algebroja ja $m \subset B$ maksimaalinen ideaali. Jos B on äärellisviritteinen, niin alkukuva $\phi^{-1}m$ on maksimaalinen ideaali algebrassa A minkä hyvänsä algebrahomomorfismin $\phi : A \to B$ suhteen.*

Todistus. Olkoon $\phi\colon A \to B$ jokin algebrahomomorfismi ja tarkastellaan kuvausta $a \mapsto \phi(a) + m : A \to B/m$. Suoraan määritelmän perusteella sen ydin on $n = \phi^{-1}m$, joten homomorfialauseen nojalla A/n on isomorfinen erään kunnan B/m alirenkaan kanssa. Siten A/n on kokonaisalue. Koska B

on äärellisviritteinen, myös B/m on äärellisviritteinen ja siis itse asiassa affiini K-alue. Niinpä B/m on edellisen lemman nojalla algebrallinen kunnan K suhteen. Silloin A/n on isomorfian perusteella algebrallinen kokonaisalue, eli edellisen lemman mukaan kunta. Siispä $n = \phi^{-1}m$ on maksimaalinen algebrassa A. □

Huomautus. Edellisen lauseen oletuksia voi lieventää: ks. sivu 35. Huomaa myös, että tuloksella on käyttökelpoinen erikoistapaus: affiinin algebran maksimaalisen ideaalin rajoittuma alialgebraan on alialgebran maksimaalinen ideaali.

Jatkoa ajatellen on hyödyllistä todistaa erillisenä lemmana seuraava yksinkertainen tulos.

Lemma 3.4. *Olkoon K kunta ja $(\xi_1, \ldots, \xi_n) \in K^n$. Tällöin polynomirenkaan $K[x_1, \ldots, x_n]$ ideaali $\langle x_1 - \xi_1, \ldots, x_n - \xi_n \rangle$ on maksimaalinen.*

Todistus. Olkoon $(\xi_1, \ldots, \xi_n) \in K^n$ ja merkitään $m = \langle x_1 - \xi_1, \ldots, x_n - \xi_n \rangle$. Olkoon $f \in K[x_1, \ldots, x_n]$ mielivaltainen polynomi,

$$f = \sum_{i=1}^{k} a_i x_1^{p_{i1}} \cdots x_n^{p_{in}}, \quad \text{missä} \quad a_1, \ldots, a_k \in K.$$

Kirjoitetaan $f = \sum_{i=1}^{k} a_i (x_1 - \xi_1 + \xi_1)^{p_{i1}} \cdots (x_n - \xi_n + \xi_n)^{p_{in}}$, jolloin f saa muodon

$$f = g + f(\xi_1, \ldots, \xi_n), \tag{3.2}$$

missä $g \in m = \langle x_1 - \xi_1, \ldots, x_n - \xi_n \rangle$. Tästä nähdään, että polynomi f on arvonsa $f(\xi_1, \ldots, \xi_n)$ kanssa kongruentti ideaalin m suhteen.

Tarkastellaan valuaatiota

$$\phi : K[x_1, \ldots, x_n] \to K, \quad \phi(f) = f(\xi_1, \ldots, \xi_n).$$

Jos $f \in \operatorname{Ker} \phi$, niin $f(\xi_1, \ldots, \xi_n) = 0$ ja näin ollen hajotelman (3.2) perusteella $f \in m$. Toisaalta, jos $f \in m$, niin saman hajotelman nojalla $f(\xi_1, \ldots, \xi_n) = 0$, eli $f \in \operatorname{Ker} \phi$. Niinpä $m = \operatorname{Ker} \phi$. Koska valuaatio on surjektio, pätee homomorfialauseen nojalla $K[x_1, \ldots, x_n]/m \simeq K$. Niinpä m on maksimaalinen ideaali. □

Olemme nyt valmiita antamaan ensimmäisen todistuksen Nullstellensatzin esimuodolle.

Lause (Nullstellensatzin esimuoto)**.** *Olkoon K algebrallisesti suljettu kunta ja $m \subset K[x_1, \ldots, x_n]$ maksimaalinen ideaali. Silloin on olemassa piste $\xi = (\xi_1, \ldots, \xi_n) \in K^n$, jolla $m = \langle x_1 - \xi_1, \ldots, x_n - \xi_n \rangle$.*

Todistus. Tarkastellaan aluksi leikkausta $K[x_i] \cap m$. Se on maksimaalisen ideaalin m alkukuva inkluusiossa $K[x_i] \hookrightarrow K[x_1, \ldots, x_n]$, joten lauseen 3.3 nojalla $K[x_i] \cap m$ on maksimaalinen algebrassa $K[x_i]$. Koska $K[x_i]$ on pääideaalialue, $K[x_i] \cap m$ on pääideaali. Lisäksi se on maksimaalisena ideaalina myös alkuideaali, joten $K[x_i] \cap m = \langle p_i \rangle_{K[x_i]}$ eräällä jaottomalla $p_i \in K[x_i]$, $\deg p_i \geq 1$. K on algebrallisesti suljettu, joten polynomilla p_i on juuri $\xi_i \in K$. Silloin $p_i = (x_i - \xi_i)q_i$ jollain $q_i \in K$, ja saadaan $\langle p_i \rangle_{K[x_i]} = \langle x_i - \xi_i \rangle_{K[x_i]}$. Erityisesti siis $x_i - \xi_i \in m$.

Edellä oleva menee läpi millä tahansa $i = 1, \ldots, n$, joten jokaiselle x_i löytyy $\xi_i \in K$, jolla $x_i - \xi_i \in m$. Määritellään ideaali m_P asettamalla

$$m_P = \langle x_1 - \xi_1, \ldots, x_n - \xi_n \rangle \subset K[x_1, \ldots, x_n]$$

ja osoitetaan, että $m_P = m$. Edellisen nojalla $m_P \subset m$, joten riittää näyttää, että myös m_P on maksimaalinen ideaali; tämä seuraa suoraan lemmasta 3.4. □

3.3 Esimuodon todistus, tapa 2

Toinen lähestymistapa perustuu paljolti kokonaisalueen ominaisuuksiin, eikä algebrojen teoriaa tarvita lainkaan. Idea pohjautuu Ritabrata Munshin vuonna 1999 julkaistuun ja J.P. Mayn muokkaamaan kekseliääseen induktiotodistukseen, joka löytyy ainakin artikkelista [7]. Lähestymistapa ei vaadi syvällisiä esitietoja eivätkä todistukset ole kovinkaan pitkiä, lukuunottamatta Munshin lauseen 3.7 todistusta, jossa on hieman enemmän työtä.

Todistetaan aluksi seuraava käytännöllinen lemma.

Lemma 3.5. *Kokonaisalueen R alkiolle $c \neq 0$ seuraavat väitteet ovat yhtäpitäviä:*

1. *Jokaiselle alkuideaalille $P \neq \{0\}$ on voimassa $c \in P$.*
2. *Jokaiselle ideaalille $I \neq \{0\}$ on olemassa $m \geq 0$, jolla $c^m \in I$.*
3. *Kokonaisalueen osamääräkunta on muotoa $R[1/c]$.*

Todistus. Valitaan aluksi jokin nollasta poikkeava alkio $c \in R$. Oletetaan nyt, että ominaisuus 1 on voimassa. Tehdään vastaoletus ja valitaan jokin nollasta poikkeava ideaali $I \subset R$, joka ei sisällä mitään alkion c potenssia. Zornin lemman perusteella on olemassa maksimaalinen tällainen ideaali P. Se ei välttämättä ole maksimaalinen renkaassa R, mutta on alkuideaali kuitenkin. Jos nimittäin $ab \in P$, mutta $a \notin P$ ja $b \notin P$, niin $P \subsetneq \langle P, a \rangle, \langle P, b \rangle$ ja silloin

$c^m \in \langle P, a\rangle$ ja $c^n \in \langle P, b\rangle$ joillakin $m, n \geq 0$. Saadaan siis esitykset $c^m = p + ra$ ja $c^n = q + sb$ eräillä $p, q \in P$ ja $r, s \in R$. Tällöin $c^{m+n} \in P$, mikä on ristiriita. Niinpä P on nollasta poikkeava alkuideaali. Se ei kuitenkaan sisällä yhtäkään alkion c potenssia, mikä on puolestaan ristiriidassa oletuksen (1) kanssa. Siis (2) pätee.

Ominaisuuden 2 vallitessa erityisesti mikä hyvänsä pääideaali $\langle b\rangle$ sisältää alkion c jonkin potenssin. Silloin $c^n = rb$ joillain $r \in R$ ja $n \geq 0$, joten osamääräkunnassa pätee $1/b = r/c^n$. Niinpä kaikki ne osamääräkunnan alkiot, joissa b on nimittäjässä, ovat kirjoitettavissa alkion $1/c$ polynomeina. Koska b oli mielivaltainen, $\mathrm{Quot}(R) \subset R[1/c]$. Toisaalta $1/c \in \mathrm{Quot}(R)$, joten sisältyminen pätee myös toiseen suuntaan. Niinpä $\mathrm{Quot}(R) = R[1/c]$.

Oletetaan sitten, että 3 pätee. Olkoon P jokin nollasta poikkeava alkuideaali ja b mikä tahansa sen alkio. Koska $\mathrm{Quot}(R) = R[1/c]$, jollain $r \in R$ ja $n \geq 0$ voidaan kirjoittaa $1/b = r/c^n$, eli $c^n = rb$. Niinpä P sisältää alkion c^n ja siten myös alkion c. □

Edellisen tuloksen avulla voidaan helposti todistaa seuraava, I. Kaplanskyn mukaan nimetty lause.

Lause 3.6 (Kaplansky)**.** *Jos R on kokonaisalue, polynomirenkaan $R[x]$ epätriviaalien alkuideaalien leikkaus on nollaideaali.*

Todistus. Olkoon $c \neq 0$ jokin alkio renkaan $R[x]$ kaikkien nollasta poikkeavien alkuideaalien leikkauksessa, vastoin väitettä. Tarkastellaan renkaiden R ja $R[x]$ osamääräkuntia

$$K = \mathrm{Quot}(R) \qquad \text{ja} \qquad L = \mathrm{Quot}(R[x]).$$

Edellisen lemman nojalla $L = R[x][1/c]$. Koska K on pienin kokonaisalueen R sisältävistä kunnista, pätee $K \subset L$. Lisäksi L sisältää alkiot x ja $1/c$, joten $K[x][1/c] \subset L$. Sisältyminen on voimassa toiseenkin suuntaan, sillä $R \subset K$ ja siten $R[x][1/c] \subset K[x][1/c]$. Niinpä $L = K[x][1/c]$.

Lemman perusteella c sisältyy renkaan $K[x]$ kaikkien nollasta poikkeavien alkuideaalien leikkaukseen. Kukin näistä on pääideaali, jonka virittäjä on alkion c alkutekijä. Alkutekijöitä ei voi olla äärettömästi, joten pääideaalialueessa $K[x]$ on vain äärellinen määrä alkuideaaleja. Silloin jaottomia alkioitakaan ei voi olla enempää, ja niinpä $K[x]$ sisältää vain äärellisen määrän jaottomia polynomeja. Jos nämä olisivat $p_1, \ldots, p_k$, niin $1 + \prod_{i=1}^{k} p_i$ olisi uusi jaoton polynomi, mikä on ristiriita. Siis vastaoletus on väärä ja väite pätee.

□

Lause 3.7 (Munshi). *Olkoon R kokonaisalue, jonka epätriviaalien alkuideaalien leikkaus on nollaideaali. Jos M on maksimaalinen ideaali renkaassa $R[x_1, \ldots, x_n]$, niin $M \cap R \neq 0$.*

Todistus tapauksessa $n = 1$. Tarkastellaan polynomirengasta $R[x]$, jossa R on oletuksen mukainen kokonaisalue. Olkoon $M \subset R[x]$ maksimaalinen ideaali ja valitaan jokin mahdollisimman pientä astetta oleva polynomi $f = a_0 + a_1 x + \ldots + a_k x^k \in M$, jossa $a_k \neq 0$. Oletetaan vastoin väitettä, että $M \cap R = 0$, eli $k \geq 1$.

Koska renkaan R epätriviaalien alkuideaalien leikkaus oletettiin nollaideaaliksi, on olemassa jokin sen alkuideaali $P \neq 0$, jolla $a_k \notin P$. Valitaan nollasta poikkeava alkio $p \in P \subset R$, jolloin vastaoletuksen mukaan $p \notin M$. Tällöin $M \subsetneq \langle M, p \rangle$, joten maksimaalisuuden perusteella on oltava $\langle M, p \rangle = R[x]$.

Merkitään $S = R \setminus P$. Jokaista $s \in S$ kohti voidaan valita jokin $m \in M$ ja mahdollisimman pientä astetta oleva polynomi $g_s(x) \in R[x]$, joilla $-s = m + pg_s(x)$ eli $pg_s(x) + s \in M$. Koska $s \notin P$, polynomi $pg_s(x) + s$ poikkeaa nollasta ja on siis vähintään astetta k kuuluessaan ideaaliin M.

Olkoon sitten $s_0 \in S$ sellainen, jolla g_{s_0} on pienintä astetta kaikista polynomeista g_s. Kirjoitetaan $g_{s_0}(x) = b_0 + b_1 x + \ldots + b_j x^j$, jossa $b_j \neq 0$ ja $j \geq k$, ja tarkastellaan polynomia

$$g(x) = a_k g_{s_0}(x) - b_j x^{j-k} f(x)$$

Nyt

$$\begin{aligned} pg(x) + a_k s_0 &= p(a_k g_{s_0}(x) - b_j x^{j-k} f(x)) + a_k s_0 \\ &= a_k(pg_{s_0}(x) + s_0) - b_j p x^{j-k} f(x) \in M \end{aligned}$$

joten g toteuttaa polynomeilta g_s vaaditun ehdon valinnalla $s = a_k s_0$. On siis oltava $\deg g \geq j$. Kuitenkin kerroin termille x^j on $a_k b_j - b_j a_k = 0$, joten g on korkeintaan astetta $j - 1$. Tämä on ristiriita, joten $M \cap R \neq 0$.

Tarkastellaan sitten tapausta $n = 2$. Olkoon $M \subset R[x, y]$ maksimaalinen ideaali, jolla $M \cap R = 0$ vastoin väitettä. Kaplanskyn lauseen nojalla $R[x]$ ja $R[y]$ toteuttavat Munshin lauseen oletukset koskien kerroinrengasta. Niinpä tapauksen $n = 1$ nojalla $R[x] \cap M$ ja $R[y] \cap M$ poikkeavat nollasta. Leikkausjoukoista voidaan siis valita mahdollisimman pientä astetta olevat polynomit $d(x)$ ja $e(y)$, missä $\deg d = m$ ja $\deg e = n$ eräillä $m, n \geq 0$.

Määritellään joukossa $\mathbb{N} \times \mathbb{N}$ järjestys $\prec$ asettamalla

$$(i, j) \prec (i', j') \quad \Leftrightarrow \quad j < j' \text{ tai jos } j = j' \text{ niin } i < i'.$$

Kyseessä on siis käänteinen leksikografinen järjestys, eli käänteinen "aakkosjärjestys". Määritellään vielä polynomin $\sum_{i,j} a_{ij} x^i y^j$ asteeksi maksimaalinen

pari (i, j) relaation $\prec$ suhteen ja nimitetään vastaavaa kerrointa johtavaksi kertoimeksi. Jos joukko $\mathbb{N} \times \mathbb{N}$ tulkitaan hilaksi koordinaatiston ensimmäisessä neljänneksessä, niin alkion seuraajat ovat kaikki sen yläpuolella olevat alkiot ja samalla rivillä kaikki sen oikealla puolella olevat alkiot.

Tarkastellaan sitten muotoa $y^j d(x)$ ja $x^i e(y)$ olevia polynomeja, missä $i, j \in \mathbb{N}$. Selvästikin niiden asteet ovat (m, j) ja (i, n). Olkoon

$$B = \{(i, j) \in \mathbb{N} \times \mathbb{N} \mid 0 \leq i \leq m \text{ ja } 0 \leq j \leq n\}$$

ja

$$\partial B = \{(i, j) \in B \mid i = m \text{ tai } j = n\}.$$

Jokaista $(i, j) \in \partial B$ kohti saadaan astetta (i, j) oleva ideaalin M alkio, nimittäin $y^j d(x)$ tai $x^i e(y)$, sen mukaan päteekö $i = m$ vai $j = n$.

Virtaus pisteestä (a_q, b_q) origoon on seuraaja-alkioiden jono

$$(0, 0) \prec (a_1, b_1) \prec \ldots \prec (a_{q-1}, b_{q-1}) \prec (a_q, b_q),$$

missä (a_{i+1}, b_{i+1}) on alkion (a_i, b_i) välitön seuraaja, eli

$$a_i = a_{i+1} - 1 \text{ ja } b_i = b_{j+1} \qquad \text{tai} \qquad a_i = a_{i+1} \text{ ja } b_i = b_{i+1} - 1.$$

Toisin sanoen piste (a_{i+1}, b_{i+1}) on joko välittömästi pisteen (a_i, b_i) ylä- tai oikealla puolella.

Olkoon $\mathcal{F}$ kaikkien virtausten joukko pisteestä (m, n) origoon. Jokaista $F \in \mathcal{F}$ kohti olkoon $M_F \subset M$ niiden polynomien joukko, joiden aste löytyy virtauksesta F. Joka tapauksessa F kulkee reunapisteen (m, n) kautta, joten aiemman nojalla M_F on epätyhjä. Huomataan myös, että M_F ei sisällä astetta $(0, 0)$ olevia polynomeja, koska $M \cap R = 0$.

Olkoon sitten $f_F \in M_F$ relaation $\prec$ mielessä mahdollisimman pientä astetta oleva polynomi, a_F sen johtava kerroin ja a alkioiden a_F tulo joukon $\mathcal{F}$ yli. Silloin $a \neq 0$, joten oletuksen nojalla löytyy alkuideaali P, joka ei sisällä alkiota a. Olkoon $p \in P$ nollasta poikkeava, jolloin $p \in R$, mutta $p \notin M$. Koska M on maksimaalinen, $\langle M, p \rangle = R[x, y]$. Olkoon $S = R \setminus P$. Koska $a \in S$, täytyy olla $a_F \in S$ jokaisella $F \in \mathcal{F}$. Mielivaltaiselle alkiolle $s \in S$ löytyy jotkin $g_s(x, y) \in R[x, y]$ ja $m \in M$, joilla $-s = pg_s(x, y) + m$ eli $pg_s(x, y) + s \in M$. Oletetaan lisäksi, että g_s on pienintä mahdollista astetta relaation $\prec$ mielessä. Huomataan, että joka tapauksessa $pg_s(x, y) + s \neq 0$, koska $s \notin P$.

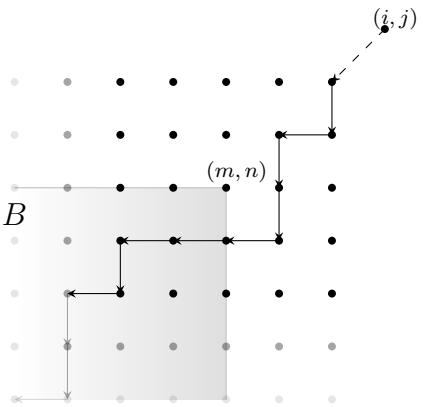
Olkoon nyt s_0 sellainen, jolla g_{s_0} on pienintä astetta kaikista valituista polynomeista g_s. Olkoon b polynomin g_{s_0} johtava kerroin ja (i, j) sen aste. Tarkastellaan mielivaltaista virtausta G pisteestä (i, j) origoon. Joka tapauksessa G sisältyy joukkoon B tai leikkaa sen reunan ∂B. Näin ollen se yhtyy

jostakin pisteestä alkaen johonkin virtaukseen pisteestä (m, n) origoon - toisin sanoen joukon $\mathcal{F}$ alkioon F. Virtaukseen F liittyvä polynomi f_F on valittu siten, että sen aste edeltää virtauksen G alkupistettä eli polynomin g_{s_0} astetta. Olkoon (u, v) näiden asteiden erotus. Silloin $x^u y^v f_F$ ja $pg_{s_0} + s_0$ ovat kaksi samanasteista ideaalin M alkiota. Niiden johtavat kertoimet voidaan saattaa samoiksi kertomalla ensimmäinen alkiolla pb ja jälkimmäinen alkiolla a_F. Koska P on alkuideaali ja alkiot a_F sekä s_0 kuuluvat sen komplementtiin, myös niiden tulo $t = a_F s_0$ on komplementissa, eli $t \in S$. Merkitään $g_t(x, y) = a_F g_{s_0}(x, y) - bx^u y^v f_F$, jolloin

$$\begin{aligned} pg_t(x, y) + t &= p(a_F g_{s_0}(x, y) - bx^u y^v f_F) + a_F s_0 \\ &= a_F(pg_{s_0}(x, y) + s_0) - bpx^u y^v f_F \in M. \end{aligned}$$

Tämä on ristiriita, sillä $g_t(x, y)$ on konstruoitu niin, että sen aste on pienempi kuin polynomin g_{s_0} aste. Niinpä vastaoletus on väärä ja väite pätee.

Munshin lause on nyt todistettu tapauksissa $n = 1$ ja $n = 2$. Muut tapaukset palautuvat näihin. □



Kuva 3.1: Eräs virtaus pisteestä (i, j) origoon

Näiden tulosten avulla olemme valmiit todistamaan Lauseen 3.1 uudella tavalla.

Lause (Nullstellensatzin esimuoto)**.** *Olkoon K algebrallisesti suljettu kunta ja $M \subset K[x_1, \ldots, x_n]$ maksimaalinen ideaali. Silloin on olemassa piste $\xi = (\xi_1, \ldots, \xi_n) \in K^n$, jolla $M = \langle x_1 - \xi_1, \ldots, x_n - \xi_n \rangle$.*

Todistus. Oletetaan, että $M \subset K[x_1, \ldots, x_n]$ on maksimaalinen ideaali. Koska K on kunta, se on kokonaisalue, ja niinpä Kaplanskyn lauseen mukaan

renkaan $K[x_i]$ alkuideaalien leikkaus on nollaideaali kaikilla $i = 1, \ldots, n$. Valitaan indekseistä jokin ja tulkitaan $K[x_1, \ldots, x_n]$ kokonaisalueen $K[x_i]$ polynomirenkaaksi

$$K[x_i][x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n].$$

Munshin lauseen nojalla $M \cap K[x_i] \neq 0$, joten voidaan poimia jokin nollasta poikkeava polynomi $f_i \in M \cap K[x_i]$. Koska K on algebrallisesti suljettu, f_i hajoaa ensimmäisen asteen tekijöihin. M on alkuideaali, joten jonkin näistä tekijöistä on kuuluttava siihen; toisin sanoen $x_i - \xi_i \in M$ eräällä $\xi_i \in K$. Löydetään siis alkiot $\xi_1, \ldots, \xi_n$, joilla

$$\langle x_1 - \xi_1, \ldots, x_n - \xi_n \rangle \subset M.$$

Tätä muotoa oleva ideaali on maksimaalinen Lemman 3.4 nojalla, joten sisältyminen ei ole aito. Siis $M = \langle x_1 - \xi_1, \ldots, x_n - \xi_n \rangle$ ja väite pätee. □

3.4 Nullstellensatzin johtaminen esimuodosta

Tässä osiossa johdetaan Nullstellensatzin heikko muoto edellä todistetusta esimuodosta 3.1. Valitun muotoilun vuoksi on syytä ensin määritellä eräs klassisen algebrallisen geometrian peruskäsite, affiini varisto.

Määritelmä 3.8. *Olkoon K kunta. Polynomikokoelmaan $S \subset K[x_1, \ldots, x_n]$ liittyvä* affiini K-varisto $\mathcal{V}(S)$ *on sen yhteisten juurten joukko, ts.*

$$\mathcal{V}(S) = \{(x_1, \ldots, x_n) \in K^n \mid f(x_1, \ldots, x_n) = 0 \quad \textit{kaikilla} \quad f \in S\}.$$

Vastaavasti, jos $X \subset K^n$ on yllä olevaa muotoa jollain $S \subset K[x_1, \ldots, x_n]$, niin sitä sanotaan affiiniksi K-varistoksi.

Luonnollisesti affiinin K-variston sijaan voidaan puhua vain affiinista varistosta, mikäli kerroinkunta on asiayhteydestä selvä.

Mainittakoon, että tässäkin kohtaa kirjallisuudessa esiintyy paljon vaihtelua terminologian suhteen. Ensinnäkin kerroinkunnan vaaditaan usein olevan algebrallisesti suljettu. Lisäksi saatettaisiin sanoa, että yllä määritelty $\mathcal{V}(S)$ on affiini algebrallinen joukko tai vain algebrallinen joukko. Silloin termi (affiini) varisto varattaisiin niille algebrallisille joukoille, joita ei voida esittää yhdisteenä kahdesta pienemmästä algebrallisesta joukosta, eli jotka ovat niin sanotusti jaottomia (engl. irreducible). Toisaalta affiini varisto saattaa tarkoittaa myös paljon yleisempää objektia, kuten algebrallisen joukon kanssa

tietyssä mielessä *isomorfista* kvasiprojektiivista avaruutta (esim. [8]). Terminologian kanssa on siis syytä olla tarkkana. Huomautettakoon vielä, ettei silti ole lainkaan tavatonta käyttää yllä valittua määritelmää (esim. [5, 6]).

Seuraavan lauseen mukaan kiinteän polynomijoukon $S \subset K[x_1, \ldots, x_n]$ sisältävät maksimaaliset ideaalit vastaavat tarkalleen affiinin variston $\mathcal{V}(S)$ alkioita, kunhan K on algebrallisesti suljettu. Tämä perustavanlaatuinen yhteys geometristen ja algebrallisten objektien välillä toimi osaltaan lähtökohtana algebrallisen geometrian esiinmarssille 1800-luvun lopulla. Tulosta saatetaan joissakin lähteissä nimittää Hilbertin Nullstellensatzin heikoksi versioksi, mutta yleensä tällä tarkoitetaan lauseesta saatavaa helppoa korollaaria.

Lause 3.9. *Olkoon K algebrallisesti suljettu kunta ja $S \subset K[x_1, \ldots, x_n]$ kokoelma polynomeja. Olkoon M_S joukon S sisältävien maksimaalisten ideaalien kokoelma. Tällöin kuvaus*

$$\Phi : \mathcal{V}(S) \to M_S, \qquad (\xi_1, \ldots, \xi_n) \mapsto \langle x_1 - \xi_1, \ldots, x_n - \xi_n \rangle$$

on hyvinmääritelty bijektio. Toisin sanoen, affiinin variston $\mathcal{V}(S)$ alkiot vastaavat täsmälleen maksimaalisia ideaaleja $m \supset S$.

Todistus. Osoitetaan ensin, että Φ on hyvinmääritelty. Olkoon $(\xi_1, \ldots, \xi_n) \in \mathcal{V}(S)$ ja $f \in S$. Manipuloimalla polynomin f esitystä saadaan

$$\begin{aligned} f(x_1, \ldots, x_n) &= f(x_1 - \xi_1 + \xi_1, \ldots, x_n - \xi_n + \xi_n) \\ &= g(x_1 - \xi_1, \ldots, x_n - \xi_n) q(x_1, \ldots, x_n) + f(\xi_1, \ldots, \xi_n), \end{aligned}$$

joillakin $g \in \langle x_1 - \xi_1, \ldots, x_n - \xi_n \rangle$ ja $q \in K[x_1, \ldots, x_n]$. Koska $(\xi_1, \ldots, \xi_n) \in \mathcal{V}(S)$, on $f(\xi_1, \ldots, \xi_n) = 0$, ja näin ollen

$$f \in \langle x_1 - \xi_1, \ldots, x_n - \xi_n \rangle = \Phi(\xi_1, \ldots, \xi_n).$$

Koska f ei riippunut pisteen $(\xi_1, \ldots, \xi_n)$ valinnasta, on $S \subset \Phi(\xi_1, \ldots, \xi_n)$. Lisäksi $\Phi(\xi_1, \ldots, \xi_n)$ on joka tapauksessa maksimaalinen Lemman 3.4 nojalla, joten $\Phi(\xi_1, \ldots, \xi_n) \in M_S$. Täten Φ on hyvinmääritelty.

Osoitetaan sitten, että Φ on bijektio näyttämällä se surjektioksi ja injektioksi. Olkoon $m \in M_S$ jokin maksimaalinen ideaali, joka sisältää kokoelman S. Nullstellensatzin esimuodon perusteella $m = \langle x_1 - \xi_1, \ldots, x_n - \xi_n \rangle$ eräällä $(\xi_1, \ldots, \xi_n) \in K^n$. Jos $f \in S$, niin $f \in m$ ja silloin $f(\xi_1, \ldots, \xi_n) = 0$. Näin ollen $(\xi_1, \ldots, \xi_n) \in \mathcal{V}(S)$, joten voidaan kirjoittaa $\Phi(\xi_1, \ldots, \xi_n) = m$. Niinpä Φ on surjektio.

Näytetään vielä, että Φ on injektio. Olkoot tätä varten $P = (\xi_1, \ldots, \xi_n)$ ja $Q = (\eta_1, \ldots, \eta_n)$ pisteitä joukossa $\mathcal{V}(S)$, joille pätee $\Phi(P) = m = \Phi(Q)$.

Nyt kuvauksen Φ määritelmän mukaan jokaisella indeksillä i on $x_i - \xi_i \in m$ ja $x_i - \eta_i \in m$, joten kaikilla i saadaan $\xi_i - \eta_i \in m$. Jos $\xi_i - \eta_i$ on kääntyvä kunnassa K, se on sitä myös renkaassa $K[x_1, \ldots, x_n]$, mikä johtaa ristiriitaan $1 \in m$. Niinpä $\xi_i = \eta_i$ jokaisella $i = 1, \ldots, n$, joten $P = Q$ ja siten Φ on injektio. □

Korollaari 3.10 (Nullstellensatz, heikko muoto)**.** *Olkoon K algebrallisesti suljettu kunta ja $I \subset K[x_1, \ldots, x_n]$ aito ideaali. Silloin*

$$\mathcal{V}(I) \neq \emptyset.$$

Todistus. Krullin lauseen nojalla I sisältyy johonkin maksimaaliseen ideaalin m. Niinpä $m \in M_I$ ja siten edellisen lauseen nojalla $\mathcal{V}(I) \neq \emptyset$. □

Nullstellensatzin mukaan polynomirenkaan aidon ideaalin alkioilla on aina yhteinen juuri, kun kerroinkunta on algebrallisesti suljettu. Esimerkiksi millä hyvänsä polynomijoukolla, joka ei sisällä vakioita, on yhteisiä juuria. Tämä antaa selityksen tuloksen nimelle, joka suomennettuna tarkoittaa ”nollakohtien teoreemaa”. Nullstellensatz on algebran peruslauseen yleistys useampaan ulottuvuuteen siinä missä kyseinen tulos takaa juuren olemassaolon renkaan $\mathbb{C}[x]$ alkioille.

Oletusten vallitessa yhteisen juuren olemassaoloon riittää siis aitousehto $I \neq K[x_1, \ldots, x_n]$, joka on *a priori* vain välttämätön. Tähän todella tarvitaan se, että K on algebrallisesti suljettu: esimerkiksi $\langle x^2 + 1 \rangle \subset \mathbb{R}[x]$ on aito ideaali, mutta sen virittäjällä ei ole yhtään juurta kunnassa $\mathbb{R}$.

3.5 Eräs suoraviivainen todistus

Tässä osiossa Nullstellensatz todistetaan suoraan, käyttämättä esimuotoa. Todistus on peräisin lähteestä [1] ja perustuu yksinkertaiseen versioon tunnetusta Noetherin normalisaatiolemmasta. Selvyyden vuoksi tarvitaan muutamia usean muuttujan polynomeihin liittyviä käsitteitä.

Olkoon K ääretön kunta ja tarkastellaan polynomia $f \in K[x_1, \ldots, x_n]$. Se on summa muotoa $kx_1^{m_1}x_2^{m_2} \cdots x_n^{m_n}$ olevista termeistä. Yhden tällaisen *aste* on eksponenttien summa $m_1 + m_2 + \ldots + m_n$ ja polynomin f *kokonaisaste* tai lyhyesti *aste* on suurin sen termien asteista. Esimerkiksi, jos f on polynomi $x_1^2x_2 + x_1x_2 + 4 \in \mathbb{R}[x_1, x_2]$, niin sen termien asteet ovat 3, 2 ja 0; niinpä polynomin aste on 3. Polynomia sanotaan *homogeeniseksi*, mikäli sen kaikki termit ovat samanasteisia. Esimerkiksi $x_1^2 + x_1x_2 + x_2^2 \in \mathbb{R}[x_1, x_2]$ on homogeeninen, $x_1^2 + x_2 \in \mathbb{R}[x_1, x_2]$ puolestaan ei. Jokainen polynomi voidaan järjestää summaksi homogeenisista komponenteista ja näin saatu esitys on luonnollisesti (järjestystä vaille) yksikäsitteinen.

Seuraava lemma on tarpeen Nullstellensatzia todistettaessa. Se on yksinkertainen versio Emmy Noetherin (1926) kuuluisasta tuloksesta.

Lemma 3.11 (Normalisaatio)**.** *Olkoon K ääretön kunta, $n \geq 2$ ja $f \in K[x_1, \ldots, x_n]$ vähintään kokonaisastetta $d = 1$ oleva polynomi. Tällöin on olemassa alkiot $\lambda_1, \ldots, \lambda_{n-1} \in K$, joilla polynomin*

$$g(x_1, \ldots, x_n) = f(x_1 + \lambda_1 x_n, x_2 + \lambda_2 x_n, \ldots, x_{n-1} + \lambda_{n-1} x_n, x_n)$$

termin x_n^d kerroin poikkeaa nollasta.

Todistus. Oletetaan, että $\lambda_1, \ldots, \lambda_{n-1} \in K$. Tarkastellaan polynomin g mielivaltaista termiä

$$k(x_1 + \lambda_1 x_n)^{m_1} \cdots (x_{n-1} + \lambda_{n-1} x_n)^{m_{n-1}} x_n^{m_n},$$

missä jokainen m_i on epänegatiivinen ja $m_1 + \ldots + m_n \leq d$. Kun tämä puretaan auki, saadaan summa astetta $m_1 + \ldots + m_n$ olevista termeistä. Näistä tarkalleen yksi sisältää vain tuntematonta x_n, nimittäin

$$k\lambda_1^{m_1} \cdots \lambda_{n-1}^{m_{n-1}} x_n^{m_1 + \ldots + m_n}. \tag{3.3}$$

Kun yhdistetään tätä muotoa olevista termeistä ne, joiden aste on d, löydetään termin x_n^d kerroin polynomissa g. Tämä on $f_d(\lambda_1, \ldots, \lambda_{n-1}, 1)$, missä f_d on polynomin f homogeeninen, d-asteinen komponentti. Oletuksen mukaan $d \geq 1$, joten $f_d(x_1, \ldots, x_{n-1}, 1) \in K[x_1, \ldots, x_{n-1}]$ ei ole nollapolynomi. Näin ollen sillä on vain äärellinen määrä juuria. Kuitenkin K on ääretön, joten on olemassa sellaiset $\lambda_1, \ldots, \lambda_{n-1} \in K$, joilla $f_d(\lambda_1, \ldots, \lambda_{n-1}, 1) \neq 0$. Tämä todistaa väitteen. □

Nyt olemme valmiit todistamaan seuraavan version Nullstellensatzista:

Lause 3.12. *Olkoon K algebrallisesti suljettu kunta ja $I \subset K[x_1, \ldots, x_n]$ aito ideaali. Tällöin on olemassa jokin $a = (a_1, \ldots, a_n) \in K^n$, jolla $f(a) = 0$ kaikilla polynomeilla $f \in I$. Toisin sanoen, $\mathcal{V}(I) \neq \emptyset$.*

Todistus. Mikäli I on nollaideaali, asia on selvä; olkoon siis $I \neq 0$. Todistetaan väite induktiolla luvun n suhteen. Tapaus $n = 1$ on helppo: Koska $K[x]$ on pääideaalialue, I on jonkin vähintään astetta 1 olevan polynomin g virittämä. Edelleen, koska K on algebrallisesti suljettu, on olemassa jokin $a \in K$, jolla $g(a) = 0$. Niinpä myös $f(a) = 0$ kaikilla $f \in I$, sillä $I = \langle g \rangle$.

Olkoon sitten $n > 1$ ja oletetaan väitteen pätevän kaikilla pienemmillä indeksin arvoilla. Lemman 3.11 perusteella voidaan olettaa, että I sisältää kokonaisastetta $e \geq 1$ olevan, muuttujan x_n suhteen pääpolynomin[1] g. Olkoon

[1] Toisin sanoen g on muotoa $g = x_n^e + P(x_1, \ldots, x_n)$, missä polynomi P ei sisällä termiä x_n^e ja on kokonaisasteeltaan korkeintaan e.

$I' \subset I$ niiden polynomien joukko, jotka eivät sisällä muuttujaa x_n. Silloin I' on renkaan $K[x_1, \ldots, x_{n-1}]$ aito ideaali ja induktio-oletuksen mukaan löytyy piste $a = (a_1, \ldots, a_{n-1}) \in K^{n-1}$, jossa jokainen ideaalin I' polynomi häviää. Muodostetaan joukko

$$J = \{f(a_1, \ldots, a_{n-1}, x_n) \mid f \in I\} \subset K[x_n]$$

ja näytetään, että se on renkaan $K[x_n]$ aito ideaali. Tämän jälkeen väite seuraa, kuten tapauksessa $n = 1$.

Tehdään vastaoletus $J = K[x_n]$ ja valitaan jokin f, jolla pätee yhtälö $f(a_1, \ldots, a_{n-1}, x_n) = 1$. Joka tapauksessa f voidaan esittää muodossa

$$f(a, x_n) = f_0(a) + f_1(a)x_n + \ldots + f_d(a)x_n^d$$

joillakin $f_i \in K[x_1, \ldots, x_{n-1}]$ ja $d \geq 1$. Jos kerran $f(a, x_n) = 1$, niin täytyy olla $f_i(a) = 0$ kaikilla $i = 1, \ldots, d$ ja $f_0(a) = 1$. Vastaavasti aiemmin valittu polynomi g voidaan kirjoittaa muodossa

$$g = g_0 + g_1 x_n + \ldots + g_{e-1}x_n^{e-1} + x_n^e$$

joillakin $g_i \in K[x_1, \ldots, x_{n-1}]$ ja $e \geq 1$.

Määritellään polynomi $R \in K[x_1, \ldots, x_{n-1}]$ polynomien f ja g kertoimien avulla seuraavanlaisena $(d + e - 1) \times (d + e - 1)$-determinanttina:

$$R = \begin{vmatrix} f_0 & f_1 & \cdots & f_d & 0 & 0 & \cdots & 0 \\ 0 & f_0 & f_1 & \cdots & f_d & 0 & \cdots & 0 \\ & & \ddots & & & & & \\ 0 & \cdots & 0 & f_0 & f_1 & \cdots & f_{d-1} & f_d \\ g_0 & g_1 & \cdots & g_{e-1} & 1 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{e-1} & 1 & 0 & 0 \\ & & \ddots & & & & \ddots & \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{e-1} & 1 \end{vmatrix} \tag{3.4}$$

Koska sarakkeen lisääminen toiseen skalaarilla kerrottuna ei vaikuta determinanttiin, on

$$R = \begin{vmatrix} f_0 + x_n f_1 + \ldots + x_n^d f_d & f_1 & \cdots & f_d & 0 & 0 & \cdots & 0 \\ x_n f_0 + \ldots + x_n^d f_{d-1} + x_n^{d+1} f_d & f_0 & f_1 & \cdots & f_d & 0 & \cdots & 0 \\ & & \ddots & & & & & \\ x_n^{e-1} f_0 + \ldots + x_n^{d+e-1} f_d & \cdots & 0 & f_0 & f_1 & \cdots & f_{d-1} & f_d \\ g_0 + x_n g_1 + \ldots + x_n^{e-1} g_{e-1} + x_n^e & g_1 & \cdots & g_{e-1} & 1 & 0 & \cdots & 0 \\ x_n g_0 + \ldots + x_n^e g_{e-1} + x_n^{e+1} & g_0 & g_1 & \cdots & g_{e-1} & 1 & 0 & 0 \\ & & \ddots & & & & \ddots & \\ x_n^d g_0 + \ldots + x_n^{d+e-1} g_{e-1} + x_n^{d+e} & \cdots & 0 & g_0 & g_1 & \cdots & g_{e-1} & 1 \end{vmatrix}$$

eli

$$R = \begin{vmatrix} f & f_1 & \cdots & f_d & 0 & 0 & \cdots & 0 \\ x_n f & f_0 & f_1 & \cdots & f_d & 0 & \cdots & 0 \\ & & \ddots & & & & & \\ x_n^{e-1} f & \cdots & 0 & f_0 & f_1 & \cdots & f_{d-1} & f_d \\ g & g_1 & \cdots & g_{e-1} & 1 & 0 & \cdots & 0 \\ x_n g & g_0 & g_1 & \cdots & g_{e-1} & 1 & 0 & 0 \\ & & \ddots & & & & \ddots & \\ x_n^d g & \cdots & 0 & g_0 & g_1 & \cdots & g_{e-1} & 1 \end{vmatrix}$$

Ensimmäisen sarakkeen suhteen kehitettynä determinantti on selvästi polynomien f ja g lineaarikombinaatio. Niinpä R kuuluu ideaaliin I. Esityksen 3.4 nojalla R ei kuitenkaan sisällä tuntematonta x_n, joten pätee $R \in I'$.

Jos determinantin määräävään matriisiin sijoitetaan vakio a, siitä tulee alakolmiomatriisi, jonka jokainen lävistäjäalkio on 1. Tunnetusti myös determinantti on tällöin 1, eli $R(a_1, \ldots, a_{n-1}) = 1$. Niinpä R ei häviäkään pisteessä $(a_1, \ldots, a_{n-1})$, mikä on ristiriita. Siis $J \subset K[x_n]$ on aito ideaali.

Rengas $K[x_n]$ on pääideaalialue, joten $J = \langle h \rangle$ jollakin polynomilla $h \in K[x_n]$. Niinpä jokaiselel $f \in J$ pätee $f = f'h$ jollakin $f' \in K[x_n]$. Koska K on algebrallisesti suljettu, virittäjälle h on olemassa juuri $a_n \in K$. Silloin

$$f(a_n) = f'(a_n)h(a_n) = 0$$

eli

$$f(a_1, \ldots, a_{n-1}, a_n) = 0.$$

□

Luku 4

Lähestymistapojen analysointia

Tähän mennessä työssä on esitetty kolme ainakin näennäisesti erilaista todistusta Nullstellensatzille. Kahdessa ensimmäisessä lähestymistavassa todistettiin ensin eräänlainen tuloksen esimuoto, kolmannessa lähestymistavassa taas kuljettiin toista kautta. Tässä osiossa tarkastellaan todistuksia ensin erikseen ja lopuksi vertaillaan toisiinsa.

4.1 Todistuksista

Ensimmäinen todistus perustuu Lauseeseen 3.3, joka puhuu maksimaalisista ideaaleista ja niiden alkukuvista. Lausetta varten on ensin todistettu kaksiosainen Lemma 3.2, jota tarvitaan kokonaisuudessaan. Lemmaa käyttämällä lauseen 3.3 todistus on yksinkertainen, mutta itse lemman todistamisessa on varsin paljon työtä. Sen ensimmäinen puolisko hoituu kivuttomasti, mutta toinen osa perustuu alkioiden matriisiesityksiin sekä jaollisuustarkasteluihin ja on varsin raskas ja tekninen. Lemman oletuksia ei voi lieventää (ks. [6], tehtävä 1.1).

Nullstellensatzin esimuodon todistuksessa Lausetta 3.3 käytetään jo alussa melko huomaamattomasti sen oleellisen seikan näyttämiseen, että leikkaus $K[x_i] \cap m$ on epätyhjä kaikilla i. Tämä on syytä huomata siksi, että seuraavassa lähestymistavassa käytetään täsmälleen samaa tulosta, mutta se perustellaan Kaplanskyn ja Munshin lauseiden avulla. Tästä eteenpäin todistukset ovat kuitenkin identtiset.

Munshin lauseeseen perustuvassa lähestymistavassa keskeisessä roolissa ovat kokonaisalueen alkuideaalit ja osamääräkunnat. Aluksi todistetaan hyödyllinen Lemma 3.5, joka karakterisoi sen ehdon, että osamääräkunta on muotoa $R[1/c]$. Tämän apulauseen todistuksessa käytetään Zornin lemmaa, mutta muuten todistus on elementaarinen.

Seuraavaksi esitettävän Kaplanskyn lauseen todistuksesta löytyy yhtymäkohtia Lemman 3.2 todistukseen. Argumentointi vaikuttaa nimittäin hyvin samanlaiselta; siinä missä aiemmassa todistuksessa puhutaan renkaasta $K[a_1, \ldots, a_r, g^{-1}]$, jälkimmäisessä on käytössä merkintä $R[x][1/c]$, ja kummassakin todistuksessa tähdätään samaan ristiriitaan.

Kaplanskyn lauseen jälkeen todistetaan Munshin lause. Sen todistus on melko tekninen jo tapauksessa $n = 1$ ja perustuu paljolti polynomien astelukujen tarkasteluihin. Tapaus $n = 2$ seuraa ensimmäisestä eräänlaisella, varsin erikoisella induktiopäättelyllä.

Näiden esivalmistelujen jälkeen päästään todistamaan Nullstellensatzin esimuotoa. Tämä tehdään käyttämällä Kaplanskyn lausetta renkaaseen $K[x_i]$, jolloin päästään soveltamaan puolestaan Munshin lausetta. Sen avulla päätellään jo edellisestä lähestymistavasta tuttu tulos, jonka mukaan $K[x_i] \cap m \neq \emptyset$ tarkastellulla maksimaalisella ideaalilla m. Kuten jo mainittu, tästä eteenpäin esimuodon todistus etenee kuten ensimmäisessä lähestymistavassa.

Kolmas lähestymistapa on hengeltään huomattavan erilainen, kuin kaksi ensimmäistä. Esimuodon sijaan tässä lähestymistavassa todistetaan Nullstellensatzin heikko versio käyttäen apuna oikeastaan vain erästä alkeellista versiota Emmy Noetherin kuuluisasta normalisaatiotuloksesta.

Lemman perusteella renkaan $K[x_1, \ldots, x_n]$ ideaaliin kuuluva polynomi antaa samaan ideaaliin kuuluvan, tuntemattoman x_n suhteen pääpolynomin, jolla on lisäksi sama kokonaisaste kuin alkuperäisellä polynomilla.

Nullstellensatzin todistus etenee induktiolla polynomialgebran indeksin suhteen. Todistuksen ydin on determinantin ominaisuuksiin perustuvassa päättelyssä. Determinantissa esiintyvän polynomin g tulee olla tuntemattoman x_n pääpolynomi ja siten sen valitsemiseen tarvittiin Lemmaa 3.11. Kyseistä determinanttia kutsutaan polynomien f ja g resultantiksi, jonka yleinen määrittely ei tässä työssä tullut tarpeelliseksi.

Muilta osin todistus on varsin yksinkertainen ja induktioväitteen todistaminen palautuu näppärästi tapaukseen $n = 1$.

4.2 Vertailua

Kaksi ensimmäistä lähestymistapaa ovat varsin samanlaisia. Ensimmäisessä käytettävälle algebrojen terminologialle on paikkansa silloin kun sille on muutakin käyttöä kontekstin puolesta, kuten esimerkiksi kirjassa [6]. Toinen lähestymistapa on tässä mielessä kevyempi ja ymmärrettävissä melko helposti hyvän algebran peruskurssin pohjalta. Kummassakin lähestymistavassa esimuotoa varten on tarpeen todistaa yksi hieman hankalampi tulos, joka ensimmäisen osalta on Lemma 3.2 ja jälkimmäisen osalta Munshin lause.

Näistä Munshin lauseen todistus on kiistatta mielenkiintoisempi ja teknisesti vähemmän vaativa, mikä edelleen puoltaa tämän lähestymistavan valitsemista monissa yhteyksissä.

Kolmas lähestymistapa lienee esitetyistä nopein. Sen yhteydessä todistettava Lemma 3.11 on kuitenkin ikävän tekninen, ja on sellaisenaan varsin rajallisesti hyödynnettävissä muissa tilanteissa. Samoin varsinainen Nullstellensatzin todistus on luonteeltaan tekninen ja varsinkin determinanttipäättelyä on vaikea esittää ilman sotkua merkintöjen kanssa. Tämä lähestymistapa lienee paikallaan esimerkiksi silloin, kun Nullstellensatz voidaan esittää teoksen liitteessä ja halutaan käyttöön ilman tarkempaa paneutumista sen perusteisiin.

Luku 5

Nullstellensatzin vahva muoto

5.1 Spektri

Nullstellensatzin vahvaa versiota varten tarvitaan hieman uusia käsitteitä ja aputuloksia. Tavoitteena on saada lause muotoiltua niin sanottujen *radikaalien* avulla. Aloitetaan kuitenkin määrittelemällä, mitä tarkoitetaan renkaan spektrillä.

Määritelmä 5.1. *Renkaan R* spektri *on sen alkuideaalien kokoelma,*

$$\mathrm{Spec}(R) = \{P \subset R \mid P \text{ alkuideaali}\}.$$

Renkaan R maksimaalinen spektri *on sen maksimaalisten ideaalien kokoelma,*

$$\mathrm{Spec}_{\max} R = \{P \subset R \mid P \text{ maksimaalinen ideaali}\}.$$

Koska kommutatiivisissa renkaissa maksimaaliset ideaalit ovat alkuideaaleja, pätee

$$\mathrm{Spec}_{\max} R \subset \mathrm{Spec}(R).$$

Tätä yksinkertaista huomiota tarvitaan myöhemmin.

Esimerkki 5.2. *Kokonaislukujen renkaan ideaalit ovat tunnetusti täsmälleen joukot $n\mathbb{Z}$, missä $n \in \mathbb{Z}$. Näistä maksimaalisia ovat alkulukujen suhteen otetut ideaalit $p\mathbb{Z}$, sillä yleisesti on voimassa*

$$n\mathbb{Z} \subset m\mathbb{Z} \quad \Leftrightarrow \quad m \mid n.$$

Toisaalta muita alkuideaaleja ei ole: jos ab on yhdistetty luku, niin $ab \in ab\mathbb{Z}$, mutta $a, b \notin ab\mathbb{Z}$, eikä $ab\mathbb{Z}$ silloin ole kommutatiivisen renkaan $\mathbb{Z}$ alkuideaali. Siispä

$$\mathrm{Spec}(\mathbb{Z}) = \{p\mathbb{Z} \mid p \text{ alkuluku}\} = \mathrm{Spec}_{\max}\mathbb{Z}.$$

Renkaan spektri on hyvin keskeisessä asemassa modernin algebrallisen geometrian näkökulmasta. Se liittyy läheisesti tunnettuun Zariskin topologiaan, jonka avulla voidaan muodostaa niin sanottuja *affiineja skeemoja*. Näitä yhdistämällä saadaan varsinaisia *skeemoja*, jotka ovat nykyaikaisen algebrallisen geometrian perusobjekteja. Skeema yleistää dramaattisesti tietynlaisen variston käsitettä, mitä varten A. Groethendick aikanaan käsitteen määrittelikin.

5.2 Radikaali

Tässä työssä skeemojen käsittely ei ole yllä olevaa tarkemmin mahdollista. Sen sijaan jatkossa tarvitaan seuraavaa algebran peruskäsitettä:

Määritelmä 5.3. *Renkaan R ideaalin I* radikaali *on*

$$\sqrt{I} = \{a \in R \mid a^n \in I \text{ jollain } n \geq 0\}.$$

Jos pätee $I = \sqrt{I}$, niin I on radikaali ideaali.

Huomautus. $\sqrt{I}$ on ideaali itsekin: jos renkaan alkioille a ja b pätee $a^n, b^m \in I$, niin $(a+b)^{n+m} \in I$ ja $(ra)^n = r^n a^n \in I$ mielivaltaisella $r \in R$. Lisäksi $\sqrt{I}$ on radikaali ideaali, eli $\sqrt{I} = \sqrt{\sqrt{I}}$, kuten sopii odottaakin: jos $a \in \sqrt{\sqrt{I}}$, jollain $n \in \mathbb{Z}$ on $a^n \in \sqrt{I}$, ja siten $a^{nm} = (a^n)^m \in I$ jollain $m \in \mathbb{Z}$. Toinen suunta on selvä, koska aina $I \subset \sqrt{I}$.

Huomaa myös, että alkuideaalit ovat radikaaleja suoraan määritelmien perusteella.

Esimerkki 5.4. *Tarkastellaan kokonaislukujen renkaan $\mathbb{Z}$ ideaalia $m\mathbb{Z}$. Määritelmän mukaan $\sqrt{m\mathbb{Z}}$ koostuu täsmälleen niistä kokonaisluvuista k, joiden jokin äärellinen potenssi k^n on jaollinen luvulla m. Mutta silloin luvun k täytyy olla jaollinen jokaisella luvun m alkutekijällä ainakin kerran. Toisaalta, jos k on tarkalleen luvun m alkutekijöiden tulo, niin jollain n pätee $m \mid k^n$, eli $k^n \in m\mathbb{Z}$. Siis $\sqrt{m\mathbb{Z}} = k\mathbb{Z}$, missä k on luvun m alkutekijöiden tulo. Esimerkiksi siis $\sqrt{12\mathbb{Z}} = 6\mathbb{Z}$, $\sqrt{64\mathbb{Z}} = 2\mathbb{Z}$ ja $\sqrt{p\mathbb{Z}} = p\mathbb{Z}$ kaikilla alkuluvuilla p.*

Toisinaan ideaalin radikaali määritellään kaikkien sen sisältävien alkuideaalien leikkaukseksi. Yllä annetun määritelmän perusteella tämä ei ole suoraan selvää ja tuloksen todistamisessa onkin hieman työtä. Aloitetaan seuraavalla lemmalla, jonka mukaan sisältyminen toiseen suuntaan on ainakin voimassa. Tuloksen voi tulkita myös niin, että ideaali ja tämän radikaali mahtuvat aina samaan alkuideaaliin.

Lemma 5.5. *Olkoon R rengas, I ideaali ja $M_I \subset \mathrm{Spec}(R)$ mielivaltainen kokoelma ideaalin I sisältäviä alkuideaaleja. Silloin*

$$\sqrt{I} \subset \bigcap_{P \in M_I} P.$$

Erityisesti

$$\sqrt{I} \subset \bigcap_{\substack{P \in \mathrm{Spec}(R), \\ I \subset P}} P.$$

Todistus. Tulos seuraa suoraan alkuideaalin ominaisuuksista: Jos $a \in \sqrt{I}$ ja P on ideaalin I sisältävä alkuideaali, niin $a^n \in I \subset P$ ja siten $a \in P$. Tämä pätee kaikilla alkuideaaleilla P, jotka sisältävät ideaalin I. Siispä a kuuluu myös näiden leikkaukseen ja väite on selvä. □

Siirtymällä hetkeksi polynomirenkaaseen $R[x]$ saadaan ideaalin radikaalille todistettua seuraava, tarkka karakterisaatio. Oivallusta kutsutaan usein Rabinowitschin keinoksi (engl. Rabinowitsch's trick) sen esiinnyttyä ensi kerran Rabinowitschin nimellä vuonna 1929 julkaistussa artikkelissa.[1]

Lause 5.6. *Olkoon R rengas ja I sen ideaali. Olkoon $M \subset \mathrm{Spec}_{\max} R[x]$ sellaisten polynomirenkaan maksimaalisten ideaalien m joukko, jotka sisältävät ideaalin I, eli joille $I \subset R \cap m$. Silloin*

$$\sqrt{I} = \bigcap_{m \in M} R \cap m$$

eli eksplisiittisemmin

$$\sqrt{I} = \bigcap_{\substack{m \in \mathrm{Spec}_{\max} R[x], \\ I \subset R \cap m}} R \cap m.$$

Todistus. Relaation $\subset$ osalta väite seuraa suoraan edellisestä lemmasta, sillä $R \cap m$ on alkuideaali kunhan m on maksimaalinen renkaassa $R[x]$. Toista suuntaa varten oletetaan, että

$$a \in \bigcap_{\substack{m \in \mathrm{Spec}_{\max} R[x], \\ I \subset R \cap m}} R \cap m.$$

Määritellään Rabinowitschin ideaa käyttäen ideaali J asettamalla

$$J = \langle I \cup \{ax - 1\} \rangle_{R[x]} \subset R[x],$$

[1] Myöhemmin on selvinnyt, että muutoin tuntematon herra Rabinowitsch olikin todellisuudessa ukrainalaissyntyinen matemaattisen fysiikan tutkija Georg Yuri Rainich.

ja näytetään, että itse asiassa $J = R[x]$. Jos $J \neq R[x]$, niin Krullin lauseen nojalla on olemassa $m \in \mathrm{Spec}_{\max} R[x]$, jolla $J \subset m$. Nyt ollaan tilanteessa

$$I \subset R \cap J \subset R \cap m,$$

joten oletuksen nojalla $a \in R \cap m$, eli erityisesti $a \in m$. Koska $ax - 1 \in J$ ja $J \subset m$, on $ax - 1 \in m$, mistä seuraa nyt $1 \in m$. Tämä on ristiriidassa sen kanssa, että $m \in \mathrm{Spec}_{\max} R[x]$, joten todella $J = R[x]$.

Käyttämällä ideaalin J määritelmää ja edellä saatua identiteettiä $J = R[x]$ löydetään kertoimet $g, g_1, \ldots, g_n \in R[x]$ ja $b_1, \ldots, b_n \in I$, joilla pätee

$$1 = \sum_{j=1}^{n} g_j b_j + g(ax - 1).$$

Teknisistä syistä tarvitsemme hetkellisesti muuttujan käänteisalkiota, mikä onnistuu helpoiten ottamalla käyttöön kuvaus

$$\phi : R[x] \to R[x, x^{-1}], \quad \phi(f(x)) = f(x^{-1}).$$

Tätä soveltamalla edellinen esitys tulee muotoon

$$1 = \sum_{j=1}^{n} \phi(g_j) b_j + \phi(g)(ax^{-1} - 1)$$

jota puolittain termillä x^k kertomalla saadaan tarvittava identiteetti

$$x^k = \sum_{j=1}^{n} x^k \phi(g_j) b_j + \phi(g)(ax^{k-1} - x^k) = \sum_{j=1}^{n} h_j b_j + h(a - x), \tag{5.1}$$

missä $h_j = x^k \phi(g_j)$ ja $h = x^{k-1}\phi(g)$. Kunhan k on suurempi kuin jokaisen polynomin g tai g_j aste, on $h_j \in R[x]$ ja $h \in R[x]$ kaikilla j, jolloin $x^k \in R[x]$. Kun sijoitetaan a tuntemattoman x paikalle yhtälöön (5.1), saadaan

$$a^k = \sum_{j=1}^{n} h_j(a) b_j.$$

Koska $h_j(a) \in R$ ja $b_j \in I$ kaikilla j, on $a^k \in I$. Siispä $a \in \sqrt{I}$, mikä oli todistettava.

□

Huomautus. Jos $m \in \mathrm{Spec}_{\max} R[x]$, niin leikkaus $R \cap m$ on todella renkaan R alkuideaali. Jos nimittäin renkaan R alkioille a ja b pätee $ab \in R \cap m$, on $ab \in m$, ja koska maksimaaliset ideaalit ovat alkuideaaleja, täytyy olla $a \in m$ tai $b \in m$. Siis $a \in R \cap m$ tai $b \in R \cap m$.

Edellisen lauseen avulla saadaan todistettua aiemmin mainittu karakterisaatio ideaalin radikaalille ideaalin sisältävien alkuideaalien leikkauksena. Toisaalta kyseessä on siis tarkennus Lemmalle 5.5.

Korollaari 5.7. *Olkoon R rengas ja I sen ideaali. Olkoon M_I ideaalin I sisältävien alkuideaalien kokoelma. Silloin*

$$\sqrt{I} = \bigcap_{P \in M_I} P \qquad \textit{eli} \qquad \sqrt{I} = \bigcap_{\substack{P \in \mathrm{Spec}(R), \\ I \subset P}} P.$$

Todistus. Edellisen lauseen mukaan

$$\sqrt{I} = \bigcap_{\substack{m \in \mathrm{Spec}_{\max} R[x], \\ I \subset R \cap m}} R \cap m.$$

Leikkaukset $R \cap m$ ovat alkuideaaleja, joten

$$\sqrt{I} \subset \bigcap_{P \in M_I} P.$$

Toinen suunta seuraa suoraan Lemmasta 5.5. □

Esimerkki 5.8. *Aiemman esimerkin mukaan kokonaislukurenkaan ideaalin $m\mathbb{Z}$ radikaali on $k\mathbb{Z}$, missä k on luvun m eri alkutekijöiden tulo. Toisaalta tiedämme, että kyseisen renkaan alkuideaalit ovat muotoa $p\mathbb{Z}$ kullakin alkuluvulla p. Koska $m\mathbb{Z} \subset p\mathbb{Z}$ jos ja vain jos $p \mid m$, ideaalin $m\mathbb{Z}$ sisältävän alkuideaalin virittäjä on jokin luvun m alkutekijä. Niinpä kaikkien tällaisten alkuideaalien leikkaus on juurikin $k\mathbb{Z}$, missä k on luvun m eri alkutekijöiden tulo.*

Affiinin algebran tapauksessa lause 5.6 voidaan esittää seuraavassa, hieman yleisemmässä muodossa. Tulos on keskeisessä roolissa todistettaessa Nullstellensatzin vahvempaa versiota.

Lause 5.9. *Olkoon A affiini algebra ja olkoon I sen ideaali. Silloin*

$$\sqrt{I} = \bigcap_{\substack{m \in \mathrm{Spec}_{\max} A, \\ I \subset m}} m,$$

eli ideaalin I radikaali saadaan sen sisältävien maksimaalisten ideaalien leikkauksena.

Todistus. Maksimaaliset ideaalit ovat alkuideaaleja, joten sisältyminen $\subset$ on selvä. Oletetaan sitten, että $n \in \mathrm{Spec}_{\max} A[x]$ ja tarkastellaan leikkausta $A \cap n$. Koska A on affiini algebra, voidaan myös $A[x]$ tulkita äärellisesti viritetyksi algebraksi kunnan yli. Silloin $A \cap n$ on Lauseen 3.3 mukaan maksimaalinen algebrassa A, eli $A \cap n \in \mathrm{Spec}_{\max} A$. Näin ollen

$$\bigcap_{\substack{m \in \mathrm{Spec}_{\max} A, \\ I \subset m}} m \subset \bigcap_{\substack{n \in \mathrm{Spec}_{\max} A[x], \\ I \subset A \cap n}} A \cap n.$$

Koska aiemman lauseen mukaan

$$\sqrt{I} = \bigcap_{\substack{n \in \mathrm{Spec}_{\max} A[x], \\ I \subset A \cap n}} A \cap n,$$

pätee siis

$$\bigcap_{\substack{m \in \mathrm{Spec}_{\max} A, \\ I \subset m}} m \subset \sqrt{I},$$

eli sisältyminen on voimassa toiseenkin suuntaan. □

Edellisen lauseen nojalla affiinit algebrat ovat ns. Jacobsonin renkaita (ks. sivu 35). Nämä muodostavat tärkeän luokan renkaiden teoriassa. Ennen Nullstellensatzin vahvan muodon käsittelyä määritellään vielä yksi algebrallisessa geometriassa keskeinen käsite.

Määritelmä 5.10. *Olkoon K kunta ja $X \subset K^n$ kokoelma pisteitä.* Joukon X ideaali $\mathcal{I}(X)$ *on niiden polynomien $f \in K[x_1, \ldots, x_n]$ joukko, jotka häviävät jokaisessa joukon X pisteessä. Toisin sanoen,*

$$\mathcal{I}(X) = \{f \in K[x_1, \ldots, x_n] \mid f(\xi_1, \ldots, \xi_n) = 0 \text{ } \textit{kaikilla} \text{ } (\xi_1, \ldots, \xi_n) \in X\}.$$

Huomautus. Joukon ideaali on aina radikaali ideaali: jos $f^n \in \mathcal{I}(X)$, niin $f^n(\xi_1, \ldots, \xi_n) = 0$ kaikilla $(\xi_1, \ldots, \xi_n) \in X$. Koska K on kokonaisalue, pätee $f(\xi_1, \ldots, \xi_n) = 0$ kaikilla $(\xi_1, \ldots, \xi_n) \in X$, eli $f \in \mathcal{I}(X)$.

5.3 Nullstellensatz

Tarvittavat käsitteet Nullstellensatzin vahvan muodon esittämiseksi ja todistamiseksi ovat nyt käytettävissä.

Lause 5.11 (Nullstellensatz)**.** *Olkoon K algebrallisesti suljettu kunta ja $I \subset K[x_1, \ldots, x_n]$ ideaali. Silloin*

$$\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}.$$

Todistus. Olkoon ensin $f \in \mathcal{I}(\mathcal{V}(I))$ ja osoitetaan, että $f \in \sqrt{I}$. Koska $K[x_1, \ldots, x_n]$ on affiini algebra, riittää näyttää, että f kuuluu jokaiseen ideaalin I sisältävään maksimaaliseen ideaaliin. Olkoon siis m maksimaalinen ideaali ja $I \subset m$. Koska K on algebrallisesti suljettu, aiemmin todistetun lauseen 3.1 mukaan $m = \langle x_1 - \xi_1, \ldots, x_n - \xi_n \rangle$ jollain $(\xi_1, \ldots, \xi_n) \in \mathcal{V}(I)$. Nyt $f(\xi_1, \ldots, \xi_n) = 0$, eli $f \in m$.

Olkoon sitten $f \in \sqrt{I}$ eli $f^k \in I$ jollain $k \geq 0$. Jos $(\xi_1, \ldots, \xi_n) \in \mathcal{V}(I)$, niin $f(\xi_1, \ldots, \xi_n)^k = 0$ ja siten $f(\xi_1, \ldots, \xi_n) = 0$. Siis $f \in \mathcal{I}(\mathcal{V}(I))$. □

Nullstellensatzin vahva muoto antaa tärkeän yhteyden algebran ja geometrian välille. Seuraava korollaari valaisee tätä yhteyttä. Sen mukaan algebrallisesti suljetun kunnan tapauksessa affiinit varistot ja polynomirenkaan radikaalit ideaalit vastaavat toisiaan järjestysrelaation kääntävän bijektion välityksellä. Tämän tyyppistä yhteyttä kutsutaan toisinaan Galois'n yhteydeksi (engl. *Galois connection*).

Korollaari 5.12. *Olkoon K algebrallisesti suljettu kunta ja $n > 0$ kokonaisluku. Silloin joukkojen $A = \{I \subset K[x_1, \ldots, x_n] \mid I \text{ radikaali ideaali}\}$ ja $B = \{X \subset K^n \mid X \text{ affiini varisto}\}$ välillä on järjestyksen kääntävä bijektio.*

Todistus. Määritellään kuvaukset $f : A \to B$ ja $g : B \to A$ asettamalla $f(I) = \mathcal{V}(I)$ sekä $g(X) = \mathcal{I}(X)$. Ensinnäkin kuvaukset ovat hyvinmääriteltyjä, joten riittää näyttää ne toistensa käänteiskuvauksiksi ja todeta järjestysominaisuus.

Jos $I \in A$ eli I on radikaali ideaali, niin Nullstellensatzin nojalla $gf(I) = \mathcal{I}(\mathcal{V}(I)) = \sqrt{I} = I$. Toisaalta, jos $X \in B$, niin $X = \mathcal{V}(S)$ jollain $S \subset K[x_1, \ldots, x_n]$. Siten $S \subset \mathcal{I}(X)$, ja saadaan

$$\mathcal{V}(\mathcal{I}(X)) \subset \mathcal{V}(S) = X \subset \mathcal{V}(\mathcal{I}(X))$$

eli $fg(X) = \mathcal{V}(\mathcal{I}(X)) = X$. Niinpä f ja g ovat toistensa käänteiskuvauksia.

Enää on näytettävä, että kuvaukset kääntävät järjestyksen. Jos $I, J \in A$ ja $I \subset J$, niin suoraan määritelmän perusteella pätee $\mathcal{V}(J) \subset \mathcal{V}(I)$. Vastaavasti, jos $X, Y \in B$ ja $X \subset Y$, niin $\mathcal{I}(Y) \subset \mathcal{I}(X)$. Niinpä ehdosta $\mathcal{V}(J) \subset \mathcal{V}(I)$ seuraa $I \subset J$ ja ehdosta $\mathcal{I}(Y) \subset \mathcal{I}(X)$ puolestaan $X = \mathcal{V}(\mathcal{I}(X)) \subset \mathcal{V}(\mathcal{I}(Y)) = Y$. Saatiin siis

$$I \subset J \qquad \Longleftrightarrow \qquad f(J) \subset f(I)$$

ja

$$X \subset Y \qquad \Longleftrightarrow \qquad g(Y) \subset g(X).$$

□

Luku 6

Erilaisia versioita Nullstellensatzista

Algebrallisen geometrian kulmakivenä Hilbertin Nullstellensatz esitetään lähestulkoon jokaisessa alan perusteita käsittelevässä teoksessa. Muotoiluja tulokselle on olemassa useita riippuen käytetyistä käsitteistä ja näkökulmista. Tässä osiossa esitän joitakin vastaantulleita, käyttökelpoisia Nullstellensatzin esitysmuotoja. Aloitetaan seuraavalla näennäisesti erilaisella versiolla Nullstellensatzin heikosta muodosta.

Lause 6.1 (Nullstellensatz, heikko muoto)**.** *Olkoon K algebrallisesti suljettu kunta ja A äärellisesti viritetty K-algebra. Jos m on tämän algebran maksimaalinen ideaali, niin A/m on isomorfinen kerroinkunnan K kanssa.*

Todistus. Joka tapauksessa A/m on kunta ja K-algebrana äärellisesti viritetty, joten Lemman 3.2 mukaan se on algebrallinen kunnan K suhteen. Se on siis tulkittavissa algebrallisesti suljetun kunnan K algebralliseksi laajennokseksi, joten täytyy olla $A/m \simeq K$. □

Tässä työssä Nullstellensatzin vahvaa muotoa lähestyttiin radikaalien kautta. Tätä terminologiaa käyttäen tulos voidaan esittää kompaktissa muodossa ja helposti muistettavana yhtälönä. Toisaalta radikaalin käsitteelle ei aina ole muuta käyttöä, jolloin on toivottavaa voida esittää tulos jossain muussa muodossa. Esimerkkinä tästä voidaan esittää seuraava muotoilu, jota käytetään ainakin tunnetussa algebrallisen geometrian perusteita käsittelevässä kirjassa [8].

Lause 6.2. *Olkoon K algebrallisesti suljettu kunta ja $X = \mathcal{V}(f_1, \ldots, f_k)$ eräillä $f_1, \ldots, f_k \in K[X_1, \ldots, X_n]$. Jos $f \in \mathcal{I}(X)$, niin $f^m \in \langle f_1, \ldots, f_k \rangle$ jollakin $m \geq 1$.*

Todistus. Hilbertin kantalauseen nojalla jokaisella ideaalilla I on äärellinen virittäjäjoukko. Tämän jälkeen tulos seuraa triviaalisti Lauseesta 5.11. □

Viimeisenä esimerkkinä esitetään Nullstellensatzin yleistetty muoto, joka tässä jätetään kuitenkin todistamatta. Tämän version esittää ainakin D. Eisenbud perusteellisessa kirjassaan [3]. Myöhempiäkin esimerkkejä varten on syytä aluksi määritellä mitä tarkoitetaan Jacobsonin renkaalla.

Määritelmä 6.3. *Rengas R on* Jacobsonin rengas*, jos sen radikaalit ideaalit ovat leikkauksia maksimaalisista ideaaleista, eli jos mielivaltaiselle ideaalille $I \subsetneq R$ pätee*

$$\sqrt{I} = \bigcap_{\substack{m \in \operatorname{Spec}_{\max} R, \\ I \subset m}} m.$$

Korollaarin 5.7 mukaan $\sqrt{I}$ on ideaalin I sisältävien alkuideaalien leikkaus. Jos jonkin renkaan alkuideaalit ovat maksimaalisia tai leikkauksia maksimaalisista ideaaleista, kyseessä on siis Jacobsonin rengas. Toisaalta sama pätee toisinkin päin: Jacobsonin renkaassa jokaiselle alkuideaalille P on voimassa

$$\sqrt{P} = \bigcap_{\substack{m \in \operatorname{Spec}_{\max} R, \\ P \subset m}} m,$$

ja koska $P = \sqrt{P}$, Jacobsonin renkaassa alkuideaalit ovat leikkauksia maksimaalisista ideaaleista. Niinpä Jacobsonin renkaan määritelmä voitaisiin korvata seuraavalla tuloksella:

Lause 6.4. *Rengas on Jacobsonin rengas, jos ja vain jos sen alkuideaalit ovat maksimaalisten ideaalien leikkauksia.*

Esimerkiksi $\mathbb{Z}$ on Jacobsonin rengas, sillä jokainen sen alkuideaali on maksimaalinen. Lauseen 5.9 perusteella myös kaikki affiinit algebrat ovat Jacobsonin renkaita.

Jacobsonin renkaita kutsutaan toisinaan myös Hilbertin renkaiksi seuraavan, varsin vahvan tuloksen myötä.

Lause 6.5 (Nullstellensatzin yleinen muoto)**.** *Olkoon R Jacobsonin rengas. Silloin myös jokainen äärellisesti viritetty R-algebra S on Jacobsonin rengas. Lisäksi jos $n \subset S$ on maksimaalinen ideaali, niin $n \cap R$ on renkaan R maksimaalinen ideaali, ja S/n on kunnan $R/(n \cap R)$ äärellinen laajennos.*

Todistus. Ks. esim. [3]. □

Huomautus. Lemman 2.1 nojalla edellinen tulos yleistää myös lausetta 3.3. Tämän enempää oletuksia ei kuitenkaan voi lieventää, mikä nähdään seuraavassa esimerkissä.

Esimerkki 6.6. *Olkoon* $R = K[t]_{\langle t \rangle}$ *renkaan* $K[t]$ *lokalisaatio alkuideaalin* $\langle t \rangle$ *suhteen. Renkaan* R *ainoa maksimaalinen ideaali on* $\langle t \rangle$*, joten alkuideaali* $\langle 0 \rangle$ *ei ole maksimaalinen eikä* R *ole Jacobsonin rengas. Jos* $n = \langle xt - 1 \rangle \subset R[x]$*, niin* $R[x]/n \simeq K(t)$*, joten* n *on maksimaalinen. Kuitenkin* $n \cap R = \langle 0 \rangle$ *eli alkukuva ei ole maksimaalinen.*

Sivulla 13 esitetty Nullstellensatzin esimuodon todistus toimii sellaisenaan yleisen muodon ollessa voimassa, sillä kunnat ovat Jacobsonin renkaita. Samoin lause 5.9 voidaan todistaa suoraan edellisestä lauseesta. Näin ollen myös lause 5.11 eli Nullstellensatzin vahva muoto seuraa yleisestä muodosta.

Luku 7

Nullstellensatzin käyttöä

Tässä osiossa esitellään joitakin algebrallisen geometrian peruskäsitteitä ja tuloksia, joiden parissa tarvitaan Nullstellensatzia. Aloitetaan määrittelemällä klassisessa algebrallisessa geometriassa hyvin keskeinen käsite, koordinaattirengas.

7.1 Koordinaattirengas

Määritelmä 7.1. *Olkoon K kunta, $X \subset K^n$ affiini varisto ja $I = \mathcal{I}(X) \subset K[x_1, \ldots, x_n]$ tämän ideaali. Variston X* koordinaattirengas *on tekijärengas*

$$K[X] = K[x_1, \ldots, x_n]/I.$$

Sitä kutsutaan myös variston X säännöllisten funktioiden renkaaksi *(engl. ring of regular functions).*

Huomautus. Jos $X = \mathcal{V}(J)$, niin saattaa olla $K[X] \neq K[x_1, \ldots, x_n]/J$. Kuitenkin, jos K on algebrallisesti suljettu, niin Nullstellensatzin mukaan $I = \mathcal{I}(\mathcal{V}(J)) = \sqrt{J}$ eli saadaan $K[X] = K[x_1, \ldots, x_n]/\sqrt{J}$.

Koordinaattirenkaan alkiot ovat luokat $f + I$, jossa $f \in K[x_1, \ldots, x_n]$ on jokin polynomi. Koska $X \subset K^n$, koordinaattirenkaan alkio määrittelee kuvauksen

$$(\xi_1, \ldots, \xi_n) \mapsto f(\xi_1, \ldots, \xi_n) : X \to K.$$

Lisäksi eri luokat $f + I$ ja $g + I$ määrittelevät välttämättä eri kuvaukset: jos $f(x) = g(x)$ kaikilla $x \in X$, niin $(f - g)(x) = 0$ kaikilla $x \in X$, ja silloin $f - g \in I = \mathcal{I}(X)$ eli $f + I = g + I$. Niinpä rengas $K[X]$ on eräiden funktioiden $X \to K$ muodostama algebra. Näitä kutsutaan säännöllisiksi funktioiksi ja ne ovat tarkalleen sellaiset funktiot $X \to K$, jotka ovat polynomin

määrittelemiä. Säännöllinen funktio on siis polynomifunktion $K^n \to K$ rajoittuma joukkoon X. Ne ovat tärkeässä roolissa algebrallisessa geometriassa ja vastaavat jatkuvia funktioita topologiassa yhtä lailla kuin sileät funktiot differentiaaligeometriassa.

7.2 Alivaristot

Variston $X \subset K^n$ *alivaristo* on osajoukko $Y \subset X$ joka on itsekin varisto, toisin sanoen renkaan $K[x_1, \ldots, x_n]$ jonkin osajoukon nollajoukko. Nullstellensatzin avulla voidaan osoittaa (ks. [6]), että algebrallisesti suljetussa kunnassa variston X alivaristot vastaavat koordinaattirenkaan $K[X]$ radikaaleja ideaaleja. Tämä vastaavuus saadaan lisäksi sisältymisrelaation kääntävän bijektion välityksellä, eli kyseessä on Galois'n yhteys, kuten korollaarissa 5.12. Rajoittumalla yhden pisteen alivaristoihin saadaan lisäksi bijektiivinen vastaavuus variston X pisteiden ja koordinaattirenkaan $K[X]$ *maksimaalisten* ideaalien välille. Tämä on hyödyllinen havainto.

7.3 Redusoidut algebrat

Renkaan alkiota r sanotaan nilpotentiksi, mikäli jokin sen potenssi häviää, eli pätee $r^n = 0$ jollakin $n \geq 1$. Nilpotenttien alkioiden kokoelmaa kutsutaan *nilradikaaliksi* (engl. nil radical) ja merkitään $\operatorname{nil} R$:

$$\operatorname{nil} R = \{r \in R \mid r^n = 0 \text{ jollakin } n \geq 1\}.$$

Nimensä mukaisesti käsite liittyy aikaisemmin määriteltyyn ideaalin radikaaliin, nimittäin $\operatorname{nil} R = \sqrt{\{0\}}$, kuten suoraan määritelmistä selviää. Toisaalta korollaarin 5.7 perusteella nilradikaali on renkaan kaikkien alkuideaalien leikkaus.

Esimerkiksi reaalisten neliömatriisien joukosta on helppo löytää nilpotentteja alkioita. Aina tällaisia ei kuitenkaan löydy, vaan esimerkiksi minkä hyvänsä kokonaisalueen nilradikaali on yksiö $\{0\}$. Tämä huomio johtaa määritelmään:

Määritelmä 7.2. *Rengas on* redusoitu*, mikäli sen nilradikaali on triviaali, eli* $\operatorname{nil} R = \{0\}$.

Koordinaattirenkaat ja redusoidut algebrat liittyvät toisiinsa seuraavan lauseen mukaisesti.

Lause 7.3. *Koordinaattirengas $K[X]$ on redusoitu ja affiini K-algebra. Lisäksi, jos K on algebrallisesti suljettu, jokainen redusoitu affiini K-algebra on isomorfinen jonkin koordinaattirenkaan $K[X]$ kanssa.*

Todistus. Jos $I = \mathcal{I}(X)$, niin $K[X] = K[x_1, \ldots, x_n]/I$, eli affiinin algebran tekijärenkaana $K[X]$ on itsekin affiini algebra. Lisäksi I on radikaali ideaali huomautuksen 5.2 nojalla, joten sen suhteen otettu tekijärengas on redusoitu: $(f + I)^n = f^n + I = I$, jos ja vain jos $f^n \in I$ eli $f \in I$.

Oletetaan sitten, että K on algebrallisesti suljettu ja A jokin redusoitu ja affiini K-algebra. Silloin $A = K[a_1, \ldots, a_n]$ joillakin $a_1, \ldots, a_n \in A$. Renkaiden homomorfialauseen nojalla kuvaus

$$f \mapsto f(a_1, \ldots, a_n) \colon K[x_1, \ldots, x_n] \to A$$

antaa isomorfian $A \simeq K[x_1, \ldots, x_n]/I$, kun I on kuvauksen ydin. Koska A on redusoitu, I on radikaali, joten jos $X = \mathcal{V}(I)$, niin Nullstellensatzin mukaan

$$I = \sqrt{I} = \mathcal{I}(\mathcal{V}(I)) = \mathcal{I}(X).$$

Siis $A \simeq K[X]$. □

Toisin sanoen algebrallisesti suljetun kunnan suhteen koordinaattirenkaat vastaavat tarkalleen redusoituja äärellisesti viritettyjä K-algebroja.

7.4 Korollaareja ja esimerkkejä

Lause 7.4. *Nullstellensatzin heikko ja vahva muoto ovat yhtäpitävät.*

Todistus. Luvussa 5 vahva muoto johdettiin heikosta muodosta Rabinowitschin keinon avulla. Toinen suunta nähdään helpommin. Jos nimittäin $\mathcal{V}(I) = \emptyset$, niin vahvan muodon pätiessä $\mathcal{I}(\mathcal{V}(I)) = K[x_1, \ldots, x_n]$ eli $\sqrt{I} = K[x_1, \ldots, x_n]$. Silloin erityisesti $1 \in \sqrt{I}$ ja edelleen $1 \in I$. Siis I ei voi olla aito ideaali. Toisin sanoen, jos vahva muoto on voimassa ja I on aito ideaali, niin $\mathcal{V}(I) \neq \emptyset$. Siis heikko muoto pätee. □

Nullstellensatzista saadaan suoraan seuraava kriteeri polynomiyhtälöryhmän ratkeavuudelle.

Korollaari 7.5. *Olkoon K algebrallisesti suljettu kunta. Yhtälöryhmällä*

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= 0 \\ &\vdots \\ f_m(x_1, \ldots, x_n) &= 0 \end{aligned}$$

ei ole ainuttakaan ratkaisua renkaassa K^n, jos ja vain jos on olemassa polynomit $p_1, \ldots, p_m \in K[x_1, \ldots, x_n]$, joilla

$$1 = \sum_{i=1}^{m} p_i f_i.$$

Todistus. Jos yhtälöryhmällä ei ole ainuttakaan ratkaisua, niin $\mathcal{V}\langle f_1, \ldots, f_m\rangle = \emptyset$, joten Nullstellensatzin heikon muodon nojalla $\langle f_1, \ldots, f_m\rangle = K[x_1, \ldots, x_n]$. Niinpä $1 \in \langle f_1, \ldots, f_m\rangle$ eli

$$1 = \sum_{i=1}^{m} p_i f_i$$

joillakin $p_i \in K[x_1, \ldots, x_n]$. Toisaalta, jos tällaiset polynomit p_i on olemassa, niin yhteisiä juuria ei voi löytyä. Silloin $\mathcal{V}\langle f_1, \ldots, f_m\rangle = \emptyset$ eli yhtälöryhmällä ei ole ratkaisua. □

Seuraava esimerkki on harjoitustehtävänä kirjassa [8].

Esimerkki 7.6. *Tarkastellaan joukkoa $X = \{(x, y) \in K^2 \mid y^2 = x^3\}$. Sen ideaali on määritelmän mukaan*

$$I_X = \{f \in K[x, y] \mid f(x, y) = 0 \text{ kaikilla } (x, y) \in X\},$$

joten $\langle y^2 - x^3\rangle \subset I_X$. Nullstellensatzin perusteella jokaiselle $f \in I_X$ pätee $f^r \in \langle y^2 - x^3\rangle$ jollakin r, eli $y^2 - x^3$ jakaa polynomin f^r. Mutta $y^2 - x^3$ on jaoton, joten tämän täytyy päteä myös arvolla $r = 1$. Niinpä $f \in \langle y^2 - x^3\rangle$, eli itse asiassa $I_X = \langle y^2 - x^3\rangle$.

Tarkastellaan sitten koordinaattirengasta $K[X] = K[x, y]/I_X$ ja valitaan jokin $f + I_X \in K[X]$. Tulkitaan f muuttujan y polynomiksi renkaan $K[x]$ yli ja käytetään jakoyhtälöä; silloin $f = (y^2 - x^3) \cdot g + r$ eräillä yksikäsitteisillä polynomeilla $g, r \in K[x][y]$, missä polynomin r aste tuntemattoman y suhteen on korkeintaan 1. Niinpä koordinaattirenkaassa pätee $f = r$, jolloin $f = P(x) + Q(x)y$ joillakin yksikäsitteisillä $P, Q \in K[x]$.

Tässä työssä on puhuttu paljon varistoista ja tutkittu niiden ominaisuuksia. Yhtään esimerkkiä variston määrittämisestä käytännössä ei kuitenkaan ole vielä annettu. Seuraava, kirjasta [6] peräisin oleva harjoitustehtävä täydentää tätä puutetta.

Esimerkki 7.7. *Tarkastellaan polynomialgebraa $\mathbb{R}[x_1, x_2]$ ja sen pääideaalia*

$$I = \left\langle x_1^4 + x_2^4 + 2x_1^2x_2^2 - x_1^2 - x_2^2\right\rangle \subset \mathbb{R}[x_1, x_2]$$

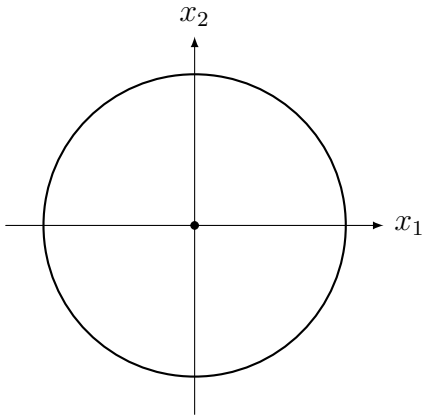
Koska

$$x_1^4 + x_2^4 + 2x_1^2x_2^2 - x_1^2 - x_2^2 = (x_1^2 + x_2^2)^2 - (x_1^2 + x_2^2) \\ = (x_1^2 + x_2^2)((x_1^2 + x_2^2) - 1),$$

niin affiini varisto $\mathcal{V}(I)$ *on origon ja yksikköympyrän yhdiste,*

$$\mathcal{V}(I) = \left\{(x_1, x_2) \in \mathbb{R}^2 \mid x_1^2 + x_2^2 = 1\right\} \cup \{(0,0)\}.$$

Koska virittäjäpolynomi hajoaa epätriviaaleihin tekijöihin, I *ei voi olla alkuideaali. Onko se kuitenkin radikaali, eli kaikkien sen sisältävien renkaan* $\mathbb{R}[x_1, x_2]$ *alkuideaalien leikkaus? Jos* I *sisältyy johonkin alkuideaaliin* P*, niin* $x_1^2 + x_2^2 \in P$ *tai* $x_1^2 + x_2^2 - 1 \in P$*. Nämä ovat molemmat jaottomia polynomeja, joten* $P = \langle x_1^2 + x_2^2 \rangle$ *tai* $P = \langle x_1^2 + x_2^2 - 1 \rangle$*. Niinpä tällaisten alkuideaalien* P *leikkaus sisältyy ideaaliin* I*, joten* I *on radikaali, eli* $I = \sqrt{I}$*. Entä sen affiinin variston ideaali* $\mathcal{I}(\mathcal{V}(I))$*, eli niiden polynomien joukko, jotka häviävät jokaisessa variston pisteessä? On selvää, että tällaisen polynomin täytyy olla jaollinen sekä polynomilla* $x_1^2 + x_2^2 - 1$ *että polynomilla* $x_1^2 + x_2^2$ *ja sisältyä näin ollen ideaaliin* I*. Toisaalta sisältyminen pätee myös toisin päin, joten* $I = \mathcal{I}(\mathcal{V}(I))$*. Niinpä tässä tapauksessa* $\sqrt{I} = \mathcal{I}(\mathcal{V}(I))$*, vaikka kerroinkunta ei olekaan algebrallisesti suljettu.*



Kuva 7.1: Esimerkin 7.7 varisto $\mathcal{V}(I)$

Kirjallisuutta

[1] Enrique Arrondo. Another elementary proof of the nullstellensatz. *The American Mathematical Monthly*, 113(2):169–171, 2006.

[2] K. Devlin. *The Joy of Sets: Fundamentals of Contemporary Set Theory.* Springer Undergraduate Texts in Mathematics and Technology. Springer New York, 1993.

[3] D. Eisenbud. *Commutative Algebra: With a View Toward Algebraic Geometry.* Graduate Texts in Mathematics. Springer, 1995.

[4] Jokke Häsä. Algebra II. luentomoniste, Helsingin Yliopisto, 2010.

[5] T.W. Hungerford. *Algebra.* Graduate Texts in Mathematics. Springer, 1974.

[6] G. Kemper. *A Course in Commutative Algebra.* Graduate Texts in Mathematics. Springer Berlin Heidelberg, 2010.

[7] J. P. May. Munshi's proof of the nullstellensatz. *American Mathematical Monthly*, 110:133–140, 2003.

[8] I.R. Shafarevich. *Basic Algebraic Geometry.* Number 1 in Basic Algebraic Geometry. Springer-Verlag, 1994.